Bitdefender ANTIVIRUS PLUS

HANDLEIDING

Bitdefender Antivirus Plus
Handleiding

Publication date 07/19/2020

Kennisgevingen

Bitdefender

Inhoudsopgave

Installatie 1

1. Voorbereiden voor installatie 2

2. Systeemvereisten 3
2.1. Softwarevereisten 3

3. Uw Bitdefender-product installeren 5
3.1. Installeren vanaf Bitdefender Central 5
3.2. Installeren vanaf de installatiedisk 8

Aan de slag 13

4. De basisfuncties 14
4.1. Open het Bitdefender-venster. 15
4.2. Notificaties 16
4.3. Profielen 17
4.3.1. Automatische activatie van profielen configureren 18
4.4. Wachtwoordbeveiligde Bitdefender-instellingen 18
4.5. Productrapporten 19
4.6. Kennisgevingen speciale aanbiedingen 20

5. Bitdefender-interface 21
5.1. Systeemvakpictogram 21
5.2. Navigatiemenu 23
5.3. Dashboard 24
5.3.1. Gebied beveiligingsstatus 24
5.3.2. Autopilot 25
5.3.3. Snelle acties 25
5.4. De Bitdefender-secties 26
5.4.1. **Beveiliging** 27
5.4.2. **Privacy** 28
5.4.3. **Hulpprogramma's** 29
5.5. Producttaal wijzigen 30

6. Bitdefender Central 31
6.1. Naar Bitdefender Central gaan 31
6.2. Twee-factorenauthenticatie 32
6.2.1. Betrouwbare apparaten toevoegen 34
6.3. Mijn abonnementen 34
6.3.1. Controleer beschikbare abonnementen 34
6.3.2. Een nieuw apparaat toevoegen 35
6.3.3. Abonnement verlengen 36
6.3.4. Abonnement activeren 36
6.4. Mijn apparaten 36
6.5. Activiteit 38
6.6. Notificaties 39

7. Bitdefender up-to-date houden 40
7.1. Controleren of Bitdefender up-to-date is 40
7.2. Een update uitvoeren 41
7.3. De automatische update in- of uitschakelen 41
7.4. De update-instellingen aanpassen 42
7.5. Doorlopende updates 43

Zo werkt het 44

8. Installatie 45
8.1. Hoe installeer ik Bitdefender op een tweede apparaat? 45
8.2. Hoe kan ik Bitdefender opnieuw installeren? 45
8.3. Waar kan ik mijn Bitdefender-product van downloaden? 46
8.4. Hoe kan ik de taal van mijn Bitdefender-product veranderen? 47
8.5. Hoe gebruik ik mijn Bitdefender-abonnement na een Windows-upgrade? 48
8.6. Hoe kan ik upgraden naar de recentste Bitdefender-versie? 50

9. Bitdefender Central 52
9.1. Hoe meldt u zich met een andere account aan voor Bitdefender-account? 52
9.2. Hoe schakel ik Bitdefender Central-hulpberichten uit? 52
9.3. Ik ben het wachtwoord dat ik voor mijn Bitdefender-account heb gekozen, vergeten. Hoe kan ik het terugstellen? 53
9.4. Hoe kan ik de aanmeldsessies van mijn Bitdefender-account beheren? 54

10. Scannen met Bitdefender 55
10.1. Een bestand of map scannen 55
10.2. Hoe kan ik mijn systeem scannen? 55
10.3. Hoe plan ik een scan? 56
10.4. Een aangepaste scantaak maken 56
10.5. Hoe sluit ik een map uit van de scan? 58
10.6. Wat moet ik doen wanneer Bitdefender een schoon bestand als geïnfecteerd beschouwt? 59
10.7. Hoe kan ik controleren welke bedreigingen Bitdefender heeft gedetecteerd? 60

11. Privacy bescherming 61
11.1. Hoe kan ik controleren of mij online transactie beveiligd is? 61
11.2. Hoe kan ik een bestand definitief verwijderen met Bitdefender? 61
11.3. Hoe kan ik versleutelde bestanden handmatig herstellen wanneer het herstelproces faalt? 62

12. Nuttige informatie 63
12.1. Hoe test ik mijn beveiligingsoplossing? 63
12.2. Hoe kan ik Bitdefender verwijderen? 63
12.3. Hoe kan ik Bitdefender VPN verwijderen? 64
12.4. Hoe verwijder ik de extensie Anti-tracker van Bitdefender? 65
12.5. Hoe kan ik de apparaat automatisch afsluiten nadat het scannen is voltooid? 66
12.6. Bitdefender configureren voor het gebruik van een proxy-internetverbinding 67
12.7. Gebruik ik een 32- of 64-bits versie van Windows? 68

12.8. Verborgen objecten weergeven in Windows ... 69
12.9. Andere beveiligingsoplossingen verwijderen ... 70
12.10. Opnieuw opstarten in Veilige modus ... 71

Uw beveiliging beheren ... 73

13. Antivirusbeveiliging ... 74
13.1. Scannen bij toegang (real time-beveiliging) ... 75
13.1.1. De real time-beveiliging in- of uitschakelen ... 75
13.1.2. De geavanceerde instellingen voor de realtime beveiliging configureren ... 75
13.1.3. De standaardinstellingen herstellen ... 79
13.2. Scannen op aanvraag ... 79
13.2.1. Een bestand of map scannen op bedreigingen ... 80
13.2.2. Een snelle scan uitvoeren ... 80
13.2.3. Een systeemscan uitvoeren ... 80
13.2.4. Een aangepaste scan configureren ... 81
13.2.5. Antivirusscanwizard ... 84
13.2.6. Scanlogboeken controleren ... 88
13.3. Automatisch scannen van verwisselbare media ... 88
13.3.1. Hoe werkt het? ... 89
13.3.2. Scan verwisselbare media beheren ... 90
13.4. Gastbestand scannen ... 90
13.5. Scanuitsluitingen configureren ... 91
13.5.1. Bestanden en mappen uitsluiten van het scannen ... 91
13.5.2. Bestandsextensies uitsluiten van scannen ... 92
13.5.3. Scanuitsluitingen beheren ... 92
13.6. Bestanden in quarantaine beheren ... 93

14. Advanced Threat Defense ... 95
14.1. Advanced Threat Defense in- of uitschakelen ... 95
14.2. Gedetecteerde kwaadwillige aanvallen controleren ... 95
14.3. Processen toevoegen aan uitzonderingen ... 96
14.4. Detectie van exploits ... 96

15. Preventie van online dreigingen ... 98
15.1. Bitdefender waarschuwt in de browser ... 99

16. Kwetsbaarheid ... 101
16.1. Uw systeem scannen op kwetsbaarheden ... 101
16.2. De automatische kwetsbaarheidsbewaking gebruiken ... 103
16.3. Wi-Fi Security Advisor ... 105
16.3.1. De meldingen van Wi-Fi Security Advisor aan- of uitzetten ... 106
16.3.2. Thuis-Wi-Fi-netwerk configureren ... 106
16.3.3. Wifinetwerk op kantoor configureren ... 107
16.3.4. Openbare Wifi ... 107
16.3.5. Informatie controleren over Wi-Fi-netwerken ... 108

17. Ransomware-remediëring ... 110
17.1. De Ransomware-remediëring in- of uitschakelen ... 110
17.2. Automatisch herstellen in- of uitschakelen ... 110

17.3. Bestanden bekijken die automatisch werden hersteld ... 110
17.4. Versleutelde bestanden handmatig herstellen ... 111
17.5. Toepassingen aan uitzonderingen toevoegen ... 112

18. Beveiliging Wachtwoordbeheerder voor uw gegevens ... 113
18.1. Maak een nieuwe Portefeuilledatabase aan ... 114
18.2. Importeer een bestaande database ... 114
18.3. De Portefeuille-database exporteren ... 115
18.4. Synchroniseer uw portefeuilles in de cloud ... 115
18.5. Uw Portefeuille-gegevens beheren ... 116
18.6. De Wachtwoordbeheerderbeveiliging in- of uitschakelen ... 117
18.7. De instellingen voor Wachtwoordbeheerder beheren ... 117

19. Anti-tracker ... 121
19.1. Interface van Anti-tracker ... 121
19.2. Anti-tracker van Bitdefender uitschakelen ... 122
19.3. Toestaan dat een website aan tracking doet ... 122

20. VPN ... 124
20.1. VPN Openen ... 124
20.2. VPN-interface ... 124
20.3. Abonnementen ... 126

21. Safepay beveiliging voor online transacties ... 127
21.1. Bitdefender Safepay™ gebruiken ... 128
21.2. Instellingen configureren ... 129
21.3. Favorieten beheren ... 130
21.4. Safepay-notificaties uitschakelen ... 131
21.5. VPN met Safepay gebruiken ... 131

22. USB Immunizer ... 132

Hulpprogramma's ... 133

23. Profielen ... 134
23.1. Werkprofiel ... 135
23.2. Filmprofiel ... 136
23.3. Gameprofiel ... 137
23.4. Openbaar Wifi-profiel ... 138
23.5. Profiel Accumodus ... 139
23.6. Realtime Optimalisering ... 140

24. Data bescherming ... 141
24.1. Bestanden definitief verwijderen ... 141

Problemen oplossen ... 143

25. Algemene problemen oplossen ... 144
25.1. Mijn systeem lijkt traag ... 144
25.2. Het scannen start niet ... 145
25.3. Ik kan een bepaalde toepassing niet meer gebruiken ... 148

25.4. Wat moet u doen wanneer Bitdefender een website, domein, IP-adres of online toepassing blokkeert die veilig is . . . 149
25.5. Bitdefender updaten bij een langzame internetverbinding . . . 150
25.6. De Bitdefender-services reageren niet . . . 150
25.7. De Autofill-functie in mijn Portefeuille werkt niet . . . 151
25.8. Het verwijderen van Bitdefender is mislukt . . . 152
25.9. Mijn systeem start niet op na het installeren van Bitdefender . . . 153

26. Bedreigingen van uw systeem verwijderen . . . 157
26.1. Noodomgeving . . . 157
26.2. Wat moet u doen wanneer Bitdefender dreigingen vindt op uw apparaat? . . . 158
26.3. Een bedreiging in een archief opruimen . . . 160
26.4. Een bedreiging in een e-mailarchief opruimen . . . 161
26.5. Wat moet ik doen als ik vermoed dat een bestand gevaarlijk is? . . . 162
26.6. Wat zijn de wachtwoordbeveiligde bestanden in het scanlogboek? . . . 162
26.7. Wat zijn de overgeslagen items in het scanlogboek? . . . 163
26.8. Wat zijn de overgecomprimeerde bestanden in het scanlogboek? . . . 163
26.9. Waarom heeft Bitdefender een geïnfecteerd bestand automatisch verwijderd? . . . 163

Contacteer ons . . . 164

27. Hulp vragen . . . 165
27.1. Telefonische ondersteuning: . . . 167

28. Online bronnen . . . 169
28.1. Ondersteuningscentrum voor Bitdefender . . . 169
28.2. Bitdefender Ondersteuningsforum . . . 170
28.3. HOTforSecurity-portaal . . . 170

29. Contactinformatie . . . 171
29.1. Webadressen . . . 171
29.2. Lokale verdelers . . . 171
29.3. Bitdefender-kantoren . . . 171

Woordenlijst . . . 175

INSTALLATIE

1. VOORBEREIDEN VOOR INSTALLATIE

Voordat u Bitdefender Antivirus Plus installeert, moet u deze voorbereidingen voltooien om ervoor te zorgen dat de installatie vlot verloopt:

- Controleer of de apparaat waarop u Bitdefenderwilt installeren, voldoet aan de minimale systeemvereisten. Als de apparaat niet aan alle systeemvereisten voldoet, wordt het Bitdefender niet geïnstalleerd, of als het toch geïnstalleerd wordt, zal het niet goed werken en zal het systeem vertragen en instabiel worden. Raadpleeg "*Systeemvereisten*" (p. 3) voor een complete lijst van systeemvereisten.
- Meld u aan bij de apparaat met een beheerdersaccount.
- Verwijder alle gelijksoortige software van de apparaat. Indien iets wordt opgemerkt tijdens het Bitdefender-installatieproces, zult u een bericht krijgen om het te verwijderen. Als u twee beveiligingsprogramma's tegelijk uitvoert, kan dit hun werking beïnvloeden en ernstige problemen met het systeem veroorzaken. Windows Defender zal uitgeschakeld zijn tijdens de installatie.
- Het wordt aanbevolen uw apparaat verbonden te laten met Internet tijdens de installatie, zelfs wanneer u vanaf een cd/dvd installeert. Indien er nieuwere versies van de toepassingsbestanden in het installatiepakket beschikbaar zijn, kan Bitdefender deze downloaden en installeren.

2. SYSTEEMVEREISTEN

U kan Bitdefender Antivirus Plus uitsluitend installeren op apparaaten met de volgende besturingssystemen:

- Windows 7 met Service Pack 1
- Windows 8
- Windows 8.1
- Windows 10

- 2,5 GB beschikbare vrije ruimte op de harde schijf (ten minste 800 MB op de systeemschijf)
- 2 GB geheugen (RAM)

Belangrijk
Systeemprestaties kunnen worden beïnvloed voor apparaten die CPU's van een oudere generatie hebben.

Opmerking
Om na te gaan welk Windows-besturingssysteem op uw apparaat wordt uitgevoerd en voor hardwaregegevens:

- In **Windows 7**, gebruikt u een rechtermuisklik op **Mijn Computer** op het bureaublad en daarna selecteert u **Eigenschappen** in het menu.
- Zoek in **Windows 8** vanuit het Windows-startscherm **Computer** (u kunt bijvoorbeeld starten met het typen van "computer", rechtstreeks in het startscherm) en rechterklik op het pictogram ervan. Zoek in **Windows 8.1**, naar **Deze computer**.

  Selecteer **Eigenschappen** in het onderste menu. Zoek in **Systeem** naar informatie over uw systeemtype.
- In **Windows 10**, typt u **Systeem** in het zoekveld in de taakbalk en klikt u op het pictogram ervan. Zoek in **Systeem** naar informatie over uw systeemtype.

2.1. Softwarevereisten

Om Bitdefender te kunnen gebruiken, evenals alle functies ervan, moet uw apparaat voldoen aan de volgende softwarevereisten:

- Microsoft Edge 40 en hoger
- Internet Explorer 10 en hoger
- Mozilla Firefox 51 en hoger

- Google Chrome 34 en hoger

3. UW BITDEFENDER-PRODUCT INSTALLEREN

U kunt Bitdefender installeren vanaf de installatiedisk of via de web installer die u naar uw apparaat kunt downloaden vanaf de Bitdefender Central.

Indien uw aankoop voor meer dan één apparaat is (u kocht bijvoorbeeld Bitdefender Antivirus Plus voor 3 PC's), herhaal het installatieproces dan en activeer uw product met dezelfde account op elke apparaat. De account die u moet gebruiken, is deze die uw actieve abonnement van Bitdefender bevat.

3.1. Installeren vanaf Bitdefender Central

Via de Bitdefender Central kunt u de installatiekit die met het aangekochte abonnement overeenkomt, downloaden. Zodra het installatieproces voltooid is, is Bitdefender Antivirus Plus geactiveerd.

Om Bitdefender Antivirus Plus te downloaden via Bitdefender Central:

1. Ga naar Bitdefender Central.
2. Selecteer het paneel **Mijn Apparaten** en klik dan op **BESCHERMING INSTALLEREN**.
3. Kies een van de twee beschikbare opties:
   - **Bescherm dit apparaat**
     a. Selecteer deze optie en selecteer dan de eigenaar van het apparaat. Als die apparaat aan iemand anders toebehoort, klik dan op de overeenstemmende knop.
     b. Sla het installatiebestand op.
   - **Bescherm andere apparaten**
     a. Selecteer deze optie en selecteer dan de eigenaar van het apparaat. Als die apparaat aan iemand anders toebehoort, klik dan op de overeenstemmende knop.
     b. Klik op **DOWNLOADLINK VERSTUREN**.
     c. Voer een e-mailadres in het overeenkomstige veld in en klik op **E-MAIL VERZENDEN**.

        De gegenereerde downloadlink is slechts 24 uur geldig. Indien de link vervalt, dient u aan de hand van dezelfde stappen een nieuwe te genereren.

d. Controleer op het apparaat waarop u uw Bitdefender-product wilt installeren het e-mailadres dat u ingevoerd hebt en klik op de overeenkomstige downloadknop.

4. Wacht tot het downloaden voltooid is en voer het installatieprogramma uit.

Bevestigen van de installatie

Bitdefender controleert eerst uw systeem om de installatie te valideren.

Als uw systeem niet voldoet aan de minimale systeemvereisten voor het installeren van Bitdefender, wordt u op de hoogte gebracht van de gebieden die moeten worden verbeterd voordat u kunt doorgaan.

Als een niet-compatibele beveiligingsoplossing of een oudere versie van Bitdefender wordt gedetecteerd, wordt u gevraagd dit van uw systeem te verwijderen. Volg de richtlijnen om de software uit uw systeem te verwijderen, zodat problemen op een later tijdstip worden vermeden. U zult mogelijk uw apparaat opnieuw moeten opstarten om het verwijderen van de gedetecteerde beveiligingsoplossingen te voltooien.

Het Bitdefender Antivirus Plus installatiepakket wordt voortdurend bijgewerkt.

Opmerking
Het downloaden van de installatiebestanden kan lang duren, vooral bij tragere internetverbindingen.

Zodra de installatie is bevestigd, verschijnt de set-upwizard. Volg de stappen om Bitdefender Antivirus Plus te installeren.

Stap 1 - Installatie Bitdefender

Voordat u verdergaat met de installatie, moet u akkoord gaan met de Abonnementsovereenkomst. Lees de Abonnementsovereenkomst grondig door: deze bevat de algemene voorwaarden voor uw gebruik van Bitdefender Antivirus Plus.

Sluit het venster als u niet akkoord gaat met deze voorwaarden. Het installatieproces wordt afgebroken en u verlaat de installatie.

In deze stap kunnen twee bijkomende taken uitgevoerd worden:

- Zorg ervoor dat de optie **Productrapporten verzenden** geactiveerd blijft. Door deze optie toe te staan, worden rapporten met informatie over uw

gebruik van het product naar de Bitdefender-servers verzonden. Deze informatie is van essentieel belang om het product te verbeteren en kan ons helpen in de toekomst een betere ervaring te verschaffen. Merk op dat deze rapporten geen vertrouwelijke informatie bevatten, zoals uw naam of IP-adres, en dat ze niet voor commerciële doeleinden zullen gebruikt worden.

- Selecteer de taal waarin u het product wenst te installeren.

Klik op **INSTALLEREN** om het installatieproces van uw Bitdefender-product te starten.

Stap 2 - Installatie bezig

Wacht tot de installatie is voltooid. Er wordt gedetailleerde informatie over de voortgang weergegeven.

Stap 3 - Installatie voltooid

Uw Bitdefender-product werd met succes geïnstalleerd.

Er wordt een overzicht van de installatie weergegeven. Als tijdens de installatie een actieve bedreiging wordt gedetecteerd en verwijderd, kan het opnieuw opstarten van het systeem nodig zijn.

Stap - Apparaatanalyse

U wordt vervolgens gevraagd of u een analyse wilt uitvoeren van uw apparaat, om te verzekeren dat het veilig is. Tijdens deze stap zal Bitdefender kritieke systeemgebieden scannen. Klik op **Apparaatanalyse starten** om het te starten.

U kunt de scaninterface verbergen door te klikken op **Scan uitvoeren op de achtergrond**. Daarna kiest u of u op de hoogte wilt worden gebracht wanneer de scan is voltooid, of niet.

Wanneer de scan voltooid is, klikt u op **Bitdefender-interface openen**.

Opmerking

Indien u de scan niet wilt laten uitvoeren, klikt u gewoon op **Overslaan**.

Stap 5 - Aan de slag

In het venster **Aan de slag** kunt u de details van uw abonnement bekijken.

Klik op **VOLTOOIEN** om naar de Bitdefender Antivirus Plus-interface te gaan.

3.2. Installeren vanaf de installatiedisk

Om Bitdefender te installeren vanaf de installatieschijf, plaatst u de schijf in het optische station.

Binnen enkele seconden moet een installatiescherm verschijnen. Volg de instructies om de installatie te starten.

Indien het installatiescherm niet verschijnt, gebruik Windows Explorer om naar de rootdirectory van de schijf te gaan en dubbelklik op het bestand autorun.exe.

Indien uw internetsnelheid traag is of uw systeem niet met het internet verbonden is, klikt u op de knop **Installeren vanaf cd/dvd**. In dat geval zal het Bitdefender-product dat op de disk beschikbaar is, geïnstalleerd worden, terwijl een nieuwere versie zal gedownload worden vanaf de Bitdefender-servers via de productupdate.

Bevestigen van de installatie

Bitdefender controleert eerst uw systeem om de installatie te valideren.

Als uw systeem niet voldoet aan de minimale systeemvereisten voor het installeren van Bitdefender, wordt u op de hoogte gebracht van de gebieden die moeten worden verbeterd voordat u kunt doorgaan.

Als een niet-compatibele beveiligingsoplossing of een oudere versie van Bitdefender wordt gedetecteerd, wordt u gevraagd dit van uw systeem te verwijderen. Volg de richtlijnen om de software uit uw systeem te verwijderen, zodat problemen op een later tijdstip worden vermeden. U zult mogelijk uw apparaat opnieuw moeten opstarten om het verwijderen van de gedetecteerde beveiligingsoplossingen te voltooien.

Opmerking

Het downloaden van de installatiebestanden kan lang duren, vooral bij tragere internetverbindingen.

Zodra de installatie is bevestigd, verschijnt de set-upwizard. Volg de stappen om Bitdefender Antivirus Plus te installeren.

Stap 1 - Installatie Bitdefender

Voordat u verdergaat met de installatie, moet u akkoord gaan met de Abonnementsovereenkomst. Lees de Abonnementsovereenkomst grondig

door: deze bevat de algemene voorwaarden voor uw gebruik van Bitdefender Antivirus Plus.

Sluit het venster als u niet akkoord gaat met deze voorwaarden. Het installatieproces wordt afgebroken en u verlaat de installatie.

In deze stap kunnen twee bijkomende taken uitgevoerd worden:

- Zorg ervoor dat de optie **Productrapporten verzenden** geactiveerd blijft. Door deze optie toe te staan, worden rapporten met informatie over uw gebruik van het product naar de Bitdefender-servers verzonden. Deze informatie is van essentieel belang om het product te verbeteren en kan ons helpen in de toekomst een betere ervaring te verschaffen. Merk op dat deze rapporten geen vertrouwelijke informatie bevatten, zoals uw naam of IP-adres, en dat ze niet voor commerciële doeleinden zullen gebruikt worden.
- Selecteer de taal waarin u het product wenst te installeren.

Klik op **INSTALLEREN** om het installatieproces van uw Bitdefender-product te starten.

Stap 2 - Installatie bezig

Wacht tot de installatie is voltooid. Er wordt gedetailleerde informatie over de voortgang weergegeven.

Stap 3 - Installatie voltooid

Er wordt een overzicht van de installatie weergegeven. Als tijdens de installatie een actieve bedreiging wordt gedetecteerd en verwijderd, kan het opnieuw opstarten van het systeem nodig zijn.

Stap - Apparaatanalyse

U wordt vervolgens gevraagd of u een analyse wilt uitvoeren van uw apparaat, om te verzekeren dat het veilig is. Tijdens deze stap zal Bitdefender kritieke systeemgebieden scannen. Klik op **Apparaatanalyse starten** om het te starten.

U kunt de scaninterface verbergen door te klikken op **Scan uitvoeren op de achtergrond**. Daarna kiest u of u op de hoogte wilt worden gebracht wanneer de scan is voltooid, of niet.

Wanneer de scan voltooid is, klikt u op **Verdergaan met account maken**.

Opmerking
Indien u de scan niet wilt laten uitvoeren, klikt u gewoon op **Overslaan**.

Stap 5 - Bitdefender-account

Als u de initiële setup hebt voltooid, verschijnt het scherm Bitdefender-account. U hebt een Bitdefender-account nodig om het product te activeren en de online functies te kunnen gebruiken. Zie "*Bitdefender Central*" (p. 31) voor meer informatie.

Ga verder volgens uw situatie.

- **Ik wil een Bitdefender-account maken**

  1. Typ de vereiste informatie in de overeenkomende velden. De gegevens die u hier opgeeft, worden vertrouwelijk behandeld. Het wachtwoord moet minstens 8 tekens lang zijn, minstens één nummer of symbool en kleine letters en hoofdletters bevatten.
  2. Voordat u verdergaat, moet u de Gebruiksvoorwaarden aanvaarden. De Gebruiksvoorwaarden bevatten de voorwaarden waaronder u Bitdefender mag gebruiken; lees ze dus grondig door.

     U kunt eveneens het Privacybeleid lezen.
  3. Klik op **ACCOUNT AANMAKEN**.

  Opmerking
  Eens de account is aangemaakt, kunt u het gebruikte e-mailadres en wachtwoord gebruiken om in te loggen op uw account op https://central.bitdefender.com, of op de Bitdefender Central-app, indien de app geïnstalleerd is op een van uw Android- of iOS-apparaten. Ga naar Google Play, zoek Bitdefender Central op en tik op de installatie-optie om de Bitdefender Central-app voor Android te installeren. Ga naar de App Store, zoek Bitdefender Central op en tik op de installatie-optie om de Bitdefender Central-app voor iOS te installeren.

- **Ik heb al een Bitdefender-account**

  1. Klik op **Aanmelden**.
  2. Voer het e-mailadres in het daarvoor bestemde veld en klik daarna op **VOLGENDE**.
  3. Voer uw wachtwoord in en klik op **AANMELDEN**.

Bent u het wachtwoord voor uw account kwijt of wilt u het gewoon opnieuw instellen:

a. Klik op **Wachtwoord vergeten?**.

b. Voer uw e-mailadres in en klik op **VOLGENDE**.

c. Controleer uw e-mailaccount, voer de beveiligingscode in die u ontvangen hebt en klik op **VOLGENDE**.

   Of u kunt in de e-mail die we naar u gestuurd hebben, klikken op **Wachtwoord wijzigen**.

d. Geef het nieuwe wachtwoord dat u wilt instellen in en geef het vervolgens opnieuw in. Klik op **OPSLAAN**.

Opmerking
Indien u al een MyBitdefender-account hebt, kunt u deze gebruiken om u aan te melden in uw Bitdefender-account. Indien u uw wachtwoord vergeten bent, moet u eerst naar https://my.bitdefender.com gaan om het terug te stellen. Gebruik daarna de aangepaste gegevens om u aan te melden bij uw Bitdefender-account.

- **Ik wil mij aanmelden met mijn Microsoft-, Facebook- of Google-account**

Om u aan te melden met uw Microsoft-, Facebook- of Google-account:

1. Selecteer de service die u wilt gebruiken. U wordt omgeleid naar de aanmeldingspagina van die service.
2. Volg de instructies die door de geselecteerde service worden gegeven om uw account te koppelen aan Bitdefender.

Opmerking
Bitdefender krijgt geen toegang tot vertrouwelijke informatie, zoals het wachtwoord van de account die u gebruikt om aan te melden of de persoonlijke informatie van uw vrienden en contactpersonen.

Stap 6 - Uw product activeren

Opmerking
Deze stap verschijnt indien u gekozen hebt om een nieuwe Bitdefender-account aan te maken in de vorige stap, of indien u zich hebt aangemeld met een account waarop een verlopen abonnement van toepassing is.

Er is een werkende internetverbinding vereist om de activering van uw product te voltooien.

Ga verder volgens uw situatie:

- Ik heb een activeringscode

  Activeer het product in dit geval door de volgende stappen te volgen:

  1. Voer de activatiecode in het veld **Ik heb een activatiecode** in en klik daarna op **VERDERGAAN**.

     Opmerking
     U vindt uw activatiecode:
     - op het cd/dvd-label.
     - op de productregistratiekaart.
     - in de online aankoop e-mail.

  2. **Ik wil graag Bitdefender evalueren**

     In dit geval kunt u het product gedurende 30 dagen gebruiken. Om met de proefperiode te starten, selecteert u **Ik heb geen abonnement, ik wil het product gratis uitproberen** en klik daarna op **VERDERGAAN**.

Stap 7 - Aan de slag

In het venster **Aan de slag** kunt u de details van uw abonnement bekijken.

Klik op **VOLTOOIEN** om naar de Bitdefender Antivirus Plus-interface te gaan.

AAN DE SLAG

4. DE BASISFUNCTIES

Nadat u Bitdefender Antivirus Plus hebt geïnstalleerd, wordt uw apparaat beschermd tegen alle types bedreigingen (zoals malware, spyware, ransomware, exploits, botnets en Trojaanse paarden).

De toepassing gebruikt de Photontechnologie om de snelheid en prestaties van het scanproces van de bedreigingen te versterken. Het werkt door de gebruikspatronen van uw systeemtoepassingen te leren om te weten wat en wanneer er moet worden gescand, om zo de invloed op de systeemprestaties te minimaliseren.

Zonder bescherming verbinden met de publieke draadloze netwerken van luchthavens, winkelcentra, cafés of hotels kan gevaarlijk zijn voor uw apparaat en uw gegevens. Dit is voornamelijk omdat fraudeurs uw activiteit kunnen volgen en het beste moment kunnen uitkiezen om uw persoonlijke gegevens te stelen, maar ook omdat iedereen uw IP-adres kan zien, waardoor uw toestel het slachtoffer kan worden van toekomstige cyberaanvallen. Installeer en gebruik de "*VPN*" (p. 124) app om dergelijke betreurenswaardige situaties te vermijden.

U kunt uw wachtwoorden en online accounts bijhouden door ze op te slaan met "*Beveiliging Wachtwoordbeheerder voor uw gegevens*" (p. 113) in een portefeuille Met één enkel hoofdwachtwoord kunt u uw privacy beschermen tegen indringers die mogelijk proberen om uw geld af te troggelen.

Om u te beschermen tegen potentiële nieuwsgierigen en spionnen wanneer uw apparaat verbonden is met een onbeveiligd netwerk, analyseert Bitdefender het beveiligingsniveau ervan en beveelt u indien nodig aan om de veiligheid van uw online activiteiten een boost te geven. Voor instructies over hoe u uw persoonlijke gegevens veilig kunt houden, verwijzen we naar "*Wi-Fi Security Advisor*" (p. 105).

Bestanden die door ransomware worden versleuteld, kunnen nu worden hersteld zonder losgeld te moeten geven. Voor informatie over hoe u versleutelde bestanden kunt herstellen, raadpleeg "*Ransomware-remediëring*" (p. 110).

Speel games of kijk films terwijl u werkt, Bitdefender kan u een voortdurende gebruikerservaring bieden door onderhoudstaken uit te stellen, onderbrekingen te elimineren en de visuele effecten van het systeem af te stellen. U kunt van dit alles profiteren door "*Profielen*" (p. 134).

Bitdefender zal de meeste beslissingen met betrekking tot de beveiliging voor u nemen en zal zelden pop-upwaarschuwingen weergeven. Details over acties die worden ondernomen en informatie over de programmabediening zijn beschikbaar in het venster Kennisgevingen. Zie "*Notificaties*" (p. 16) voor meer informatie.

Het is aanbevolen Bitdefender af en toe te openen en eventuele bestaande problemen te herstellen. U zult mogelijk specifieke Bitdefender-componenten moeten configureren of preventieve acties ondernemen om uw apparaat en gegevens te beschermen.

Om de online functies van Bitdefender Antivirus Plus te gebruiken en uw abonnementen en toestellen te beheren, gaat u naar uw Bitdefender-account. Zie "*Bitdefender Central*" (p. 31) voor meer informatie.

In het "Zo werkt het" (p. 44) deel vindt u stap-voor-stap instructies over het uitvoeren van vaak voorkomende taken. Indien u problemen ondervindt bij het gebruik van Bitdefender, controleer dan het "*Algemene problemen oplossen*" (p. 144)deel met mogelijke oplossingen voor de problemen die het vaakst voorkomen.

4.1. Open het Bitdefender-venster.

Om naar de hoofdinterface van Bitdefender Antivirus Plus te gaan, klikt u op het pictogram op uw desktop.

Indien nodig kunt u ook de onderstaande stappen volgen:

- In **Windows 7**:
  1. Klik op **Start** en ga naar **Alle Programma's**.
  2. Klik op **Bitdefender**.
  3. Klik op **Bitdefender Antivirus Plus** of, sneller, dubbelklik op het pictogram van Bitdefender in het systeemvak.
- In **Windows 8 en Windows 8.1**:

  Zoek Bitdefender vanuit het Windows-startscherm (u kunt bijvoorbeeld beginnen met het typen van "Bitdefender", rechtstreeks in het startscherm) en klik op het pictogram ervan. U kunt ook de Desktop-app openen en dubbelklikken op het pictogram van Bitdefender in het systeemvak.
- In **Windows 10**:

Typ "Bitdefender" in het zoekveld in de taakbalk en klik dan op het pictogram ervan. Een andere mogelijkheid is het dubbelklikken op het pictogram van Bitdefender in het systeemvak.

Meer informatie over het Bitdefender-venster en -pictogram in het systeemvak, vindt u op "*Bitdefender-interface*" (p. 21).

4.2. Notificaties

Bitdefender houdt een gedetailleerd logboek bij van gebeurtenissen met betrekking tot de activiteiten van uw apparaat. Wanneer er iets belangrijks gebeurt met de veiligheid van uw systeem of gegevens, wordt er een nieuw bericht toegevoegd aan Kennisgevingen van het Bitdefender, net zoals er nieuwe e-mails verschijnen in uw Postvak IN.

Kennisgevingen zijn een belangrijk hulpmiddel bij het bewaken en beheren van uw Bitdefender-beveiliging. U kunt bijvoorbeeld heel gemakkelijk controleren of een update is geslaagd, of er bedreigingen of kwetsbaarheden op uw apparaat werden aangetroffen enz. Daarnaast kunt u zo nodig verdere acties ondernemen of acties die door Bitdefender zijn ondernomen, wijzigen.

Klik in het navigatiemenu in de Bitdefender-interface op **Notificaties** om de Notificatielog te bekijken. Telkens wanneer zich een kritiek evenement voordoet, kunt u een teller opmerken op het 2 -pictogram.

Afhankelijk van het type en de ernst worden kennisgevingen gegroepeerd in:

- **Kritieke** gebeurtenissen wijzen op kritieke problemen. U moet ze onmiddellijk controleren.
- Gebeurtenissen van het type **Waarschuwing** wijzen op niet-kritieke problemen. U moet ze controleren en herstellen wanneer u tijd hebt.
- Gebeurtenissen van het type **Informatie** duiden op een geslaagde bewerking.

Klik op elke tab om meer details te lezen over de gegenereerde gebeurtenissen. Er wordt beperkte informatie weergegeven als u een keer op elke titel van een gebeurtenis klikt, namelijk: een korte beschrijving, de actie die Bitdefender heeft ondernomen wanneer ze zich voordeed en de datum en tijd van de gebeurtenis. Er kunnen opties worden geboden voor het ondernemen van verdere actie.

Om u te helpen geregistreerde gebeurtenissen gemakkelijker te beheren, biedt het venster Kennisgevingen opties waarmee alle gebeurtenissen in dat deel kunnen worden verwijderd of gemarkeerd als gelezen.

4.3. Profielen

Sommige computeractiviteiten, zoals online games of videopresentaties, vereisen een hoger reactievermogen en hoge prestaties van het systeem zonder onderbrekingen. Wanneer uw laptop werkt op batterijvermogen, is het aanbevolen minder dringende bewerkingen die extra stroom zullen verbruiken, worden uitgesteld tot de laptop opnieuw op de netstroom is aangesloten.

Bitdefender Profielen kent meer systeemvermogen toe aan de toepassingen die worden uitgevoerd door de beveiligingsinstellingen tijdelijk te veranderen en de systeemconfiguratie aan te passen. Als gevolg daarvan is de systeeminvloed op uw activiteit beperkt.

Om zich aan verschillende activiteiten aan te passen, komt Bitdefender met de volgende profielen:

Werkprofiel
: Optimaliseert uw werk op efficiënte wijze door het product en de systeeminstellingen te herkennen en aan te passen.

Filmprofiel
: Versterkt visuele effecten en elimineert onderbrekingen bij het kijken naar films.

Gameprofiel
: Versterkt visuele effecten en elimineert onderbrekingen bij het spelen van games.

Openbaar Wifi-profiel
: Past productinstellingen toe om te genieten van volledige bescherming, terwijl u verbonden bent met een onveilig draadloos netwerk.

Profiel Accumodus
: Past productinstellingen toe en houdt achtergrondactiviteit tegen om uw accuduur te verlengen.

4.3.1. Automatische activatie van profielen configureren

Voor een gebruiksvriendelijke ervaring kunt u Bitdefender configureren om uw werkprofiel te beheren. In dit geval detecteert Bitdefender automatisch de activiteit die u uitvoert en past systeem- en productoptimalisatie-instellingen toe.

Wanneer u de **Profielen** voor het eerst opent, wordt u gevraagd om automatische profielen te activeren. Om dat te doen, klikt u gewoon op **INSCHAKELEN** in het weergegeven venster.

U kunt ook klikken op **NU NIET** indien u de voorziening op een later tijdstip wilt inschakelen.

Om Bitdefender toe te laten profielen automatisch te activeren:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Hulpprogramma's**.
2. Klik in het tabblad **Profielen** op **Instellingen**.
3. Gebruik de bijhorende schakelaar om **Profielen automatisch activeren** in te schakelen.

Indien u niet wenst dat de Profielen automatisch worden geactiveerd, zet u de schakelaar uit.

Schakel de overeenstemmende schakelaar in om een profiel manueel te activeren. Van de eerste drie profielen kan er slechts één tegelijkertijd handmatig worden geactiveerd.

Voor meer informatie over Profielen, ga naar"*Profielen*" (p. 134)

4.4. Wachtwoordbeveiligde Bitdefender-instellingen

Als u niet de enige persoon met beheermachtigingen bent die deze apparaat gebruikt, raden wij u aan uw Bitdefender-instellingen te beveiligen met een wachtwoord.

Wachtwoordbescherming configureren voor de Bitdefender-instellingen:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Instellingen**.
2. Schakel in het venster **Algemeen Wachtwoordbescherming** in.
3. Voer het wachtwoord in de twee velden in en klik op **OK**. Het wachtwoord moet minstens 8 tekens lang zijn.

Zodra u een wachtwoord hebt ingesteld, zal iedereen die de Bitdefender-instellingen probeert te wijzigen, eerst het wachtwoord moeten opgeven.

Belangrijk

Zorg dat u uw wachtwoord onthoudt of bewaar het op een veilige plaats. Als u het wachtwoord vergeten bent, moet u het programma opnieuw installeren of contact opnemen met Bitdefender voor ondersteuning.

Wachtwoordbeveiliging verwijderen:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Instellingen**.
2. Schakel in het venster **Algemeen Wachtwoordbescherming** uit.
3. Voer het wachtwoord in en klik op **OK**.

Opmerking

Klik op **Wachtwoord wijzigen** om het wachtwoord van uw product te wijzigen. Voer uw huidige wachtwoord in en klik op **OK**. In het nieuwe venster dat verschijnt, voert u het nieuwe wachtwoord in dat u voortaan wenst te gebruiken om de toegang tot uw Bitdefender-instellingen te beperken.

4.5. Productrapporten

Productrapporten bevatten informatie over hoe u het Bitdefender-product dat u geïnstalleerd hebt, gebruikt. Deze informatie is van essentieel belang om het product te verbeteren en kan ons helpen u in de toekomst een betere ervaring te bieden.

Deze rapporten bevatten geen vertrouwelijke gegevens, zoals uw naam of IP-adres, en worden niet gebruikt voor commerciële doeleinden.

Indien u tijdens de installatieprocedure hebt beslist om dergelijke rapporten naar de Bitdefender-servers te versturen en dit nu wilt stopzetten:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Instellingen**.
2. Klik op het tabblad **Geavanceerd**.
3. **Productrapporten** uitschakelen.

4.6. Kennisgevingen speciale aanbiedingen

Wanneer er reclameaanbiedingen beschikbaar zijn, is het Bitdefender product zo ingesteld dat u daarvan op de hoogte wordt gesteld via een pop-upvenster. Dit geeft u de mogelijkheid om te profiteren van voordelige tarieven en om uw apparaten beveiligd te houden gedurende een langere periode.

Om kennisgevingen voor speciale aanbiedingen in of uit te schakelen:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Instellingen**.
2. Schakel de overeenkomende schakelaar in venster **Algemeen** in of uit.

De optie speciale aanbiedingen en productmeldingen is standaard ingeschakeld.

5. BITDEFENDER-INTERFACE

Bitdefender Antivirus Plus voldoet niet alleen aan de behoeften van beginnende computergebruikers, maar ook aan de eisen van bijzonder technische gebruikers. De grafische gebruikersinterface is ontworpen zodat elke categorie gebruikers deze probleemloos kunnen gebruiken.

Om door de Bitdefender-interface te gaan, wordt een inleidingswizard getoond met informatie over hoe u moet omgaan met het product en hoe u het moet configureren. Dit wordt in de linkerbovenhoek weergegeven. Selecteer het juiste pijltje om de gids voort te zetten of **Rondleiding overslaan** om de wizard te sluiten.

Het Bitdefender-systeemvakpictogram is altijd beschikbaar, ongeacht of u het hoofdvenster wilt openen, een productupdate wilt uitvoeren of informatie wilt bekijken over de geïnstalleerde versie.

Het hoofdvenster geeft informatie over uw beveiligingsstatus. Op basis van het gebruik en de noden van uw apparaat geeft Autopilot hier verschillende soorten aanbevelingen weer om u te helpen de beveiliging en prestaties van uw apparaat te verbeteren. En u kunt de snelle acties die u het vaakst gebruikt, toevoegen, zodat u ze altijd bij de hand hebt.

Vanuit het navigatiemenu aan de linkerzijde, kunt u naar de secties instellingen, notificaties en Bitdefender gaan voor gedetailleerde configuratietaken en geavanceerde administratieve taken.

Vanuit het bovengedeelte van de hoofdinterface hebt u toegang tot uw Bitdefender-account. U kunt ons ook contacteren voor ondersteuning indien u vragen hebt of indien er iets onverwacht gebeurt.

5.1. Systeemvakpictogram

Om het volledige product sneller te beheren, kunt u het Bitdefender-pictogram in het systeemvak gebruiken.

Opmerking

Het pictogram Bitdefender is mogelijk niet altijd zichtbaar. Het pictogram permanent zichtbaar maken:

- In **Windows 7, Windows 8 en Windows 8.1**:

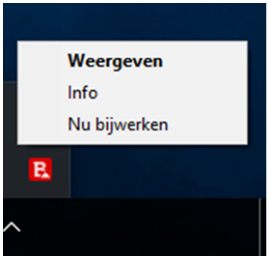
  1. Klik onderaan rechts op het scherm op de pijl.

2. Klik op **Aanpassen...** om het venster met de systeemvakpictogrammen te openen.
3. Selecteer de optie **Pictogrammen en meldingen weergeven** voor het pictogram **Bitdefender-agent**.

- In **Windows 10**:

1. Klik met de rechtermuisknop op de taakbalk en selecteer **Taakbalkinstellingen**.
2. Scroll omlaag en klik op de link **Selecteer welke iconen op de taakbalk verschijnen** onder **Systeemvak**.
3. Schakel de schakelaar naast **Bitdefender Agent** in.

Wanneer u dubbelklikt op dit pictogram, wordt Bitdefender geopend. Door met de rechterknop op het pictogram te klikken, verschijnt een snelmenu waarmee u het Bitdefender-product snel kunt beheren.



Systeemvakpictogram

- **Weergeven** - opent het hoofdvenster van Bitdefender.
- **Over** - opent een venster met informatie over Bitdefender, over waar u hulp vindt in geval van problemen en waar u de Abonnementsovereenkomst, Onderdelen van Derde partijen alsook ons Privacybeleid kunt bekijken.
- **Update nu** - start een directe update. U kunt de updatestatus volgen in het paneel Update van het hoofdvenster van Bitdefender.

Het systeemvakpictogram van Bitdefender brengt u door middel van een speciaal pictogram op de hoogte van problemen die uw apparaat beïnvloeden of van de manier waarop het product werkt. Deze symbolen zijn de volgende:

Er zijn geen problemen die de beveiliging van uw systeem beïnvloeden.
Kritieke problemen beïnvloeden de beveiliging van uw systeem. Ze vereisten uw onmiddellijke aandacht en moeten zo snel mogelijk worden hersteld.

Als Bitdefender niet werkt, verschijnt het systeemvakpictogram op een grijze achtergrond: . Dit doet zich doorgaans voor wanneer het lidmaatschap vervalt. Dit kan ook optreden wanneer de Bitdefender-services niet reageren of wanneer andere fouten de normale werking van Bitdefender beïnvloeden.

5.2. Navigatiemenu

Aan de linkerzijde van de Bitdefender-interface vindt u het navigatiemenu waarmee u snel toegang krijgt tot alle Bitdefender-functies en -tools om uw product te beheren. De beschikbare tabbladen in dit gebied zijn:

- **Dashboard**. Van hier kunt u beveiligingsproblemen snel oplossen, aanbevelingen naargelang uw systeemnoden en gebruikspatronen weergeven en snelle acties uitvoeren.
-
- **Bescherming**. Hier kunt u antivirusscans starten en configureren, gegevens herstellen indien ze werden versleuteld door ransomware en bescherming configureren wanneer u surft online.
- **Privacy**. Hier kunt u wachtwoordbeheerders maken voor uw online accounts, online betalingen in een veilige omgeving uitvoeren en de VPN-app openen.
- **Hulpprogramma's**. Hier kunt u profielen beheren en de voorziening Gegevensbescherming openen.
- **Kennisgevingen**. Van hieruit hebt u toegang tot de gegenereerde kennisgevingen.
- **Instellingen**. Van hieruit hebt u toegang tot de algemene instellingen.

Bovenaan in de interface vindt u de voorzieningen **Mijn account** en **Ondersteuning**.

- **Ondersteuning**. Van hieruit kunt u, wanneer u hulp nodig hebt bij het aanpakken van een probleem met uw Bitdefender Antivirus Plus, contact opnemen met de Technische ondersteuning van Bitdefender.
- **Mijn account**. Van hier kunt u naar uw Bitdefender-account gaan om uw abonnementen te controleren en beveiligingstaken uit te voeren op de toestellen die u beheert. Er zijn eveneens details beschikbaar over de Bitdefender-account en de lopende abonnementen.

5.3. Dashboard

Via het Dashboardvenster kunt u algemene taken uitvoeren, snel beveiligingsproblemen oplossen, informatie over het productgebruik weergeven en naar de panelen gaan van waar u de productinstellingen kunt configureren.

U kunt het allemaal met slechts enkele klikken op de knop.

Het venster is geordend in drie hoofdgebieden:

Gebied beveiligingsstatus
: Hier controleert u de beveiligingsstatus van uw apparaat.

Autopilot
: Hier kunt u de aanbevelingen voor Autopilot nagaan om de juiste werking van het systeem te verzekeren.

Snelle acties
: Hier kunt u verschillende taken lanceren om uw systeem beschermd te houden.

5.3.1. Gebied beveiligingsstatus

Bitdefender gebruikt een systeem voor het opsporen van problemen en brengt u op de hoogte van de problemen die de veiligheid van uw apparaat en gegevens kunnen beïnvloeden. De gedetecteerde problemen bevatten belangrijke beveiligingsinstellingen die worden uitgeschakeld en andere omstandigheden die een beveiligingsrisico kunnen betekenen.

Wanneer problemen de beveiliging van uw apparaat aantasten, verandert de status die aan de bovenzijde van de Bitdefender-interface staat, naar rood. De weergegeven status geeft de aard van de problemen aan die uw systeem aantasten. Daarnaast verandert de systeemvak-pictogram naar  en als u de muiscursor over het pictogram beweegt, verschijnt er een pop-up die bevestigt dat er problemen zijn.

Vermits de gedetecteerde problemen kunnen verhinderen dat Bitdefender u tegen bedreigingen beschermt of een belangrijk beveiligingsrisico kunnen inhouden, raden we aan dat u aandachtig bent en de problemen zo snel mogelijk oplost. Klik op de knop naast het gedetecteerde probleem om het probleem op te lossen.

5.3.2. Autopilot

Bitdefender Autopilot handelt als uw persoonlijke beveiligingsadviseur om u tijdens uw verschillende activiteiten een effectieve werking en verbeterde bescherming te bieden. Bitdefender Autopilot biedt contextuele aanbevelingen op basis van uw toestelgebruik en -noden, naargelang de activiteiten die u uitvoert: werken, online betalingen uitvoeren, films bekijken of games spelen. De voorgestelde aanbevelingen kunnen ook betrekking hebben op acties die u moet uitvoeren om ervoor te zorgen dat uw product aan volle capaciteit blijft werken.

Klik op de overeenkomende knop om de voorgestelde functie in gebruik te nemen of om verbeteringen door te voeren.

Autopilot-notificaties uitschakelen

Om uw aandacht te vestigen op de Autopilot-aanbevelingen, is het Bitdefender-product zo ingesteld om u via een pop-up op de hoogte te brengen.

Om de Autopilot-notificaties uit te schakelen:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Instellingen**.
2. Schakel in het venster **Algemeen** de **Aanbevelingsnotificaties** uit.

5.3.3. Snelle acties

Met snelle acties kunt u taken opstarten die u belangrijk vindt om uw systeem te beschermen en om de manier waarop u werkt, te verbeteren.

Bitdefender biedt standaard enkele snelle acties die u kunt vervangen met de acties die u zelf het vaakst gebruikt. Om een snelle actie te vervangen:

1. Klik op het pictogram in de rechterbovenhoek van de kaart die u wilt verwijderen.
2. Wijs de taak aan die u aan de hoofdinterface wilt toevoegen en klik op **TOEVOEGEN**.

De taken die u aan de hoofdinterface kunt toevoegen, zijn:

- **Snelle scan**. Voer een snelle scan uit om mogelijke bedreigingen op uw apparaat onmiddellijk te detecteren.
- **Systeemscan**. Voer een systeemscan uit om er zeker van te zijn dat uw apparaat vrij is van bedreigingen.

- **Analyse op Kwetsbaarheden**. Scan uw apparaat op kwetsbaarheden om zeker te zijn dat alle geïnstalleerde toepassingen, samen met het Besturingssysteem, bijgewerkt zijn en correct werken.
- **Wifi Beveiligingsadviseur**. Open het venster Wifi Beveiligingsadviseur binnen de module Kwetsbaarheid.
- **Portefeuilles**. Uw portefeuilles weergeven en beheren.
- **Safepay openen**. Open Bitdefender Safepay™ om uw gevoelige gegevens te beschermen terwijl u online transacties uitvoert.
- **VPN openen**. Open Bitdefender VPN om een bijkomende beschermingslaag toe te voegen wanneer u verbonden bent met het internet.
- **Bestandsvernietiging**. Start de tool Bestandsvernietiging op om sporen van gevoelige gegevens van uw apparaat te verwijderen.

Om bijkomende toestellen te beginnen beschermen met Bitdefender:

1. Klik op **Een ander apparaat installeren**.

   Er verschijnt een nieuw venster op uw scherm.

2. Klik op **DOWNLOADLINK DELEN**.

3. Volg de stappen op het scherm om Bitdefender te installeren.

Afhankelijk van uw keuze zullen de volgende Bitdefender-producten geïnstalleerd worden:

- Bitdefender Antivirus Plus op Windows-apparaten.
- Bitdefender-antivirus voor Mac op macOS X-apparaten.
- Bitdefender Mobiele beveiliging op Android-gebaseerde toestellen.
- Bitdefender Mobiele beveiliging op iOS-apparaten.

5.4. De Bitdefender-secties

Het product van Bitdefender heeft drie secties, verdeeld in nuttige functies om u te helpen beveiligd te blijven terwijl u werkt, op het web surft of online betalingen uitvoert, de snelheid van uw systeem verbetert en nog veel meer.

Wanneer u naar de functies voor een specifiek gedeelte wilt gaan of uw product wilt configureren, gaat u naar de volgende iconen in het navigatiemenu van de Bitdefender-interface:

- Beveiliging
- Privacy

-  Hulpprogramma's

5.4.1. Beveiliging

In het gedeelte Bescherming kunt u uw geavanceerde beveiligingsinstellingen configureren, de voorzieningen voor Online Threat Prevention instellen, potentiële systeemkwetsbaarheden controleren en oplossen en de beveiliging van de draadloze netwerken waarmee u verbinding maakt, beoordelen.

De functies die u in het Beveiligingsgedeelte kunt beheren, zijn:

ANTIVIRUS

Antivirusbescherming is de basis van uw beveiliging. Bitdefender beschermt u in real time en op aanvraag tegen elk type bedreiging, zoals malware, Trojaanse paarden, spyware, adware enz.

Via de Antivirusfunctie krijgt u gemakkelijk toegang tot de volgende scantaken:

- Snelle scan
- Systeemscan
- Scans beheren
- Noodomgeving

Raadpleeg "*Antivirusbeveiliging*" (p. 74) voor meer informatie over scantaken en het configureren van de antivirusbeveiliging.

ONLINE THREAT PREVENTION

Online Threat Prevention helpt u om beschermd te blijven tegen phishing-aanvallen, fraudepogingen en lekken van privégegevens terwijl u op het internet surft.

Meer informatie over het configureren van Bitdefender om uw webactiviteit te beschermen, vindt u op "*Preventie van online dreigingen*" (p. 98).

ADVANCED THREAT DEFENSE

Geavanceerde Dreigingsverdediging beschermt uw systeem actief tegen bedreigingen zoals ransomware, spyware en Trojaanse paarden door het gedrag van alle geïnstalleerde toepassingen te analyseren. Verdachte processen worden geïdentificeerd en indien nodig geblokkeerd.

Voor meer informatie over hoe u uw systeem beschermd houdt tegen bedreigingen, lees "*Advanced Threat Defense*" (p. 95).

KWETSBAARHEID

De Kwetsbaarheidsfunctie helpt u om uw besturingssysteem en de applicaties die u regelmatig gebruikt, up-to-date te houden en onveilige draadloze netwerken waarmee u een verbinding maakt, in het licht te stellen. Klik op **Openen** in de module Kwetsbaarheden om de voorzieningen ervan te openen.

Met de **Kwetsbaarheidsscan** kunt u kritieke Windows-updates, updates van toepassingen, zwakke wachtwoorden van Windows-accounts en draadloze netwerken die niet beveiligd zijn, identificeren. Klik op **Scan starten** om een scan uit te voeren voor uw apparaat.

Klik op **Wi-Fi-beveiligingsadviseur** om de lijst te bekijken van de draadloze netwerken waarmee u een verbinding maakt, samen met onze reputatiebeoordeling voor elk daarvan en de actie die u kunt ondernemen om veilig te blijven voor potentiële nieuwsgierigen.

Meer informatie over het configureren van de kwetsbaarheidsbeveiliging vindt u onder "*Kwetsbaarheid*" (p. 101).

RANSOMWARE-REMEDIËRING

De functie Ransomware-remediëring helpt u bestanden herstellen indien ze door ransomware worden versleuteld.

Voor meer informatie over hoe u versleutelde bestanden kunt herstellen, raadpleeg "*Ransomware-remediëring*" (p. 110).

5.4.2. Privacy

In het onderdeel Privacy kunt u de Bitdefender VPN-app openen, uw online transacties beschermen en uw browsingervaring veilig houden.

De functies die u in het Privacygedeelte kunt beheren, zijn:

VPN

VPN beveiligt uw online activiteit en verbergt uw IP-adres telkens u verbindt met onbeveiligde draadloze netwerken in luchthavens, winkelcentra, cafés of hotels. U kunt bovendien ook inhoud bekijken die in bepaalde gebieden afgeschermd wordt.

Voor meer informatie over deze functie, raadpleeg "*VPN*" (p. 124).

Wachtwoordmanager

Bitdefender is de wachtwoordbeheerder die helpt om uw wachtwoorden bij te houden, uw privacy beveiligt en een veilige online surfervaring verschaft.

Meer informatie over het configureren van Wachtwoordbeheerder, vindt u onder "*Beveiliging Wachtwoordbeheerder voor uw gegevens*" (p. 113).

SAFEPAY

De Bitdefender Safepay™ browser helpt u om uw online bankieren, e-shopping en alle andere soorten online transacties privé en veilig te houden.

Meer informatie over Bitdefender Safepay™ vindt u onder "*Safepay beveiliging voor online transacties*" (p. 127).

ANTI-TRACKER

De functie Anti-tracker helpt u om tracering te vermijden zodat uw data privé blijven terwijl uw browser online is. Het verkort ook de tijd die nodig is om websites te laden.

Raadpleeg voor meer informatie over de functie Anti-tracker "*Anti-tracker*" (p. 121) .

5.4.3. Hulpprogramma's

Data bescherming

Bitdefender Bestandsvernietiging helpt om gegevens permanent te verwijderen door ze fysisch te wissen van uw harde schijf.

Voor meer informatie hierover, raadpleegt u "*Data bescherming*" (p. 141).

Profielen

Dagelijkse werkactiviteiten, films kijken of games spelen kan het systeem vertragen, met name wanneer ze tegelijkertijd worden uitgevoerd met het Windows-updateproces en onderhoudstaken.

Met Bitdefender kunt u nu uw voorkeursprofiel kiezen en toepassen. Het maakt systeemafstellingen om de prestaties van specifieke geïnstalleerde toepassingen te verbeteren.

Voor meer informatie over deze functie, raadpleeg "*Profielen*" (p. 134).

5.5. Producttaal wijzigen

De interface van Bitdefender is beschikbaar in meerdere talen. U kunt de taal aan de hand van de volgende stappen aanpassen:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Instellingen**.
2. Klik in het venster **Algemeen** op **Taal wijzigen**.
3. Selecteer de gewenste taal uit de lijst en klik op **OPSLAAN**.
4. Wacht even tot de instellingen toegepast zijn.

6. BITDEFENDER CENTRAL

Bitdefender Central is het platform waar u toegang hebt tot de online functies en diensten van het product en waar u vanop afstand belangrijke taken kunt uitvoeren op apparaat waarop Bitdefender is geïnstalleerd. U kunt inloggen op uw Bitdefender-account vanop om het even welke apparaat die met het internet is verbonden via https://central.bitdefender.com of rechtstreeks vanuit de Bitdefender Central-toepassing op Android- en iOS-apparaten.

Om de Bitdefender Central-toepassing op uw apparaten te installeren:

- **Op Android** - zoek Bitdefender Central op Google Play en download en installeer de toepassing. Volg de nodige stappen om de installatie te voltooien.
- **Op iOS** - zoek Bitdefender Central in de App Store en download en installeer de toepassing. Volg de nodige stappen om de installatie te voltooien.

Zodra u aangemeld bent, kunt u beginnen met het volgende:

- Bitdefender downloaden en installeren op besturingssystemen Windows, macOS, iOS en Android. De producten die beschikbaar zijn om te downloaden, zijn:
  - Bitdefender Antivirus Plus
  - Bitdefender Antivirus voor Mac
  - Bitdefender Mobile Security voor Android
  - Bitdefender Mobile Security voor iOS
- Uw Bitdefender-abonnementen beheren en vernieuwen.
- Nieuwe apparaten aan uw netwerk toevoegen en deze apparaten beheren, waar u op dat moment ook bent.

6.1. Naar Bitdefender Central gaan

Er bestaan verschillende manieren om naar Bitdefender Central te gaan:

- Vanuit het hoofdvenster van Bitdefender:
  1. Klik in het navigatiemenu in de Bitdefender-interface op **Mijn account**.
  2. Klik op **Ga naar Bitdefender Central**.

3. Meld u aan bij uw Bitdefender-account met uw e-mailadres en wachtwoord.

- Vanuit uw webbrowser:
  1. Open een webbrowser op een computer of mobiel apparaat met internettoegang.
  2. Ga naar https://central.bitdefender.com.
  3. Meld u aan bij uw Bitdefender-account met uw e-mailadres en wachtwoord.
- Vanaf uw Android- of iOS-apparaat:

  Open de Bitdefender Central-toepassing die u geïnstalleerd hebt.

Opmerking
In dit materiaal leest u de opties en instructies die op het webplatform beschikbaar zijn.

6.2. Twee-factorenauthenticatie

De 2-Factor authenticatiemethode voegt een extra veiligheidslaag toe aan uw Bitdefender account, door een authenticatiecode te vragen bovenop uw aanmeldgegevens. Op deze manier voorkomt u dat uw account wordt overgenomen en houdt u types cyberaanvallen, zoals keyloggers, bruteforce- of woordenlijstaanvallen, af.

Twee-factorenauthenticatie activeren

Door de tweefactorenauthenticatie te activeren, maakt u uw Bitdefender account veel veiliger. Uw identiteit zal gecontroleerd worden telkens u zich aanmeldt via verschillende apparaten, hetzij om één van de Bitdefender producten te installeren, hetzij om de status van uw abonnement te controleren of vanop afstand taken uit te voeren op uw apparaten.

Om de twee-factorenauthenticatie te activeren:

1. Ga naar Bitdefender Central.
2. Klik bovenaan rechts op het scherm op de icoon .
3. Klik op **Bitdefender Account** in het schuifmenu.
4. Selecteer het tabblad **Wachtwoord en beveiliging**.
5. Klik op **Twee-factorenauthenticatie**.

6. Klik op **STARTEN**.

   Kies een van de volgende methodes:

   - **Authenticator App** - gebruik een authenticator app om een code te genereren telkens u zich wilt aanmelden op uw Bitdefender account.

     Als u een authenticator app zou willen, gebruiken, maar u niet zeker weet welke te kiezen, is er een lijst beschikbaar van de authentication apps die we aanbevelen.

     a. Klik op **AUTHENTICATOR APP GEBRUIKEN** om te starten.

     b. Om u aan te melden op een op Android of iOS gebaseerd apparaat, gebruik dat dan om de QR code te scannen.

        Om u aan te melden op een laptop of computer, kunt u de getoonde code manueel toevoegen.

        Klik op **VERDERGAAN**.

     c. Voer de code in die de app geeft of deze die weergegeven wordt in de vorige stap en klik dan op **ACTIVEREN**.

   - **E-mail** - telkens u zich aanmeldt in uw Bitdefender account, zal er een verificatiecode naar het Postvak-IN van uw e-mail worden gestuurd. Controleer uw e-mailaccount, en tik dan de code in die u hebt ontvangen.

     a. Klik op **E-MAIL GEBRUIKEN** om te starten.

     b. Controleer uw e-mailaccount en tik de verstrekte code in.

        Let erop dat u vijf minuten hebt om uw e-mailaccount te controleren en tik de gegenereerde code in. Als de tijd verstreken is, zult u een nieuwe code moeten genereren volgens dezelfde stappen.

     c. Klik op **Activeren**.

     d. U krijgt tien activeringscodes. U kunt de lijst kopiëren, downloaden of afdrukken en deze gebruiken in het geval u uw e-mailadres verliest of u zich niet meer kunt aanmelden. Elke code kan slechts eenmaal worden gebruikt.

     e. Klik op **GEREED**.

In het geval u wilt stoppen met het gebruik van de twee-factorenauthenticatie:

1. Klik op **TWEE-FACTORENAUTHENTICATIE UITSCHAKELEN**.
2. Controleer uw app of e-mailaccount en tik de code in die u hebt ontvangen.

In het geval u ervoor hebt gekozen om de authenticatiecode te ontvangen via e-mail, hebt u vijf minuten om uw e-mailaccount te controleren en de gegenereerde code in te tikken. Als de tijd verstreken is, zult u een nieuwe code moeten genereren volgens dezelfde stappen.

3. Bevestig uw keuze.

6.2.1. Betrouwbare apparaten toevoegen

Om ervoor te zorgen dat alleen u toegang hebt tot uw Bitdefender account, is het mogelijk dat we eerst een veiligheidscode vragen. Als u deze stap zou willen overslaan telkens u verbinding maakt vanaf hetzelfde apparaat, raden we u aan dit te benoemen als een betrouwbaar apparaat.

Om toestellen toe te voegen als betrouwbare apparaten:

1. Ga naar Bitdefender Central.
2. Klik bovenaan rechts op het scherm op de icoon .
3. Klik op **Bitdefender Account** in het schuifmenu.
4. Selecteer het tabblad **Wachtwoord en beveiliging**.
5. Klik op **Betrouwbare apparaten**.
6. De lijst van de apparaten waar Bitdefender op geïnstalleerd is, wordt weergegeven. Klik op het gewenste apparaat.

U kunt zo veel apparaten toevoegen als u wilt, op voorwaarde dat Bitdefender erop geïnstalleerd is en uw abonnement geldig is.

6.3. Mijn abonnementen

Via het Bitdefender Central-platform beheert u heel eenvoudig de abonnementen die u voor uw apparaten hebt aangeschaft.

6.3.1. Controleer beschikbare abonnementen

Zo controleert u uw beschikbare abonnementen:

1. Ga naar Bitdefender Central.
2. Ga naar het paneel **Mijn abonnementen**.

Hier vindt u informatie over de beschikbaarheid van uw abonnementen en het aantal apparaten dat gebruikmaakt van deze abonnementen.

U kunt een nieuw apparaat aan een abonnement toevoegen of een abonnement verlengen door een abonnementskaart te selecteren.

Opmerking
U kunt een of meer lidmaatschappen op uw account hebben, op voorwaarde dat ze voor verschillende platforms bestemd zijn (Windows, macOS, iOS of Android).

6.3.2. Een nieuw apparaat toevoegen

Indien uw abonnement meer dan één toestel dekt, kunt u een nieuw toestel toevoegen en uw Bitdefender Antivirus Plus erop installeren, als volgt:

1. Ga naar Bitdefender Central.
2. Selecteer het paneel **Mijn Apparaten** en klik dan op **BESCHERMING INSTALLEREN**.
3. Kies een van de twee beschikbare opties:
   - **Bescherm dit apparaat**

     Selecteer deze optie en selecteer dan de eigenaar van het apparaat. Als die apparaat aan iemand anders toebehoort, klik dan op de overeenstemmende knop.
   - **Bescherm andere apparaten**

     Selecteer deze optie en selecteer dan de eigenaar van het apparaat. Als die apparaat aan iemand anders toebehoort, klik dan op de overeenstemmende knop.

     Klik op **DOWNLOADLINK VERSTUREN**. Voer een e-mailadres in het overeenkomstige veld in en klik op **E-MAIL VERZENDEN**. De gegenereerde downloadlink is slechts 24 uur geldig. Indien de link vervalt, dient u aan de hand van dezelfde stappen een nieuwe te genereren.

     Controleer op het apparaat waarop u uw Bitdefender-product wilt installeren het e-mailadres dat u ingevoerd hebt en klik op de overeenkomstige downloadknop.
4. Wacht tot het downloaden voltooid is en voer het installatieprogramma uit.

6.3.3. Abonnement verlengen

Indien u automatische verlenging voor uw Bitdefender-abonnement hebt uitgeschakeld, kunt u het handmatig verlengen via de volgende stappen:

1. Ga naar Bitdefender Central.
2. Ga naar het paneel **Mijn abonnementen**.
3. Selecteer de gewenste abonnementskaart.
4. Klik op **VERNIEUWEN** om door te gaan.

In uw webbrowser wordt een webpagina geopend waar u uw Bitdefender-abonnement kunt verlengen.

6.3.4. Abonnement activeren

Een abonnement kan geactiveerd worden tijdens het installatieproces als u uw Bitdefender-account gebruikt. Samen met het activeringsproces begint het aftellen van de geldigheid.

Indien u een activeringscode hebt gekocht bij een van onze verdelers of als geschenk hebt ontvangen, kunt u de beschikbaarheid ervan toevoegen aan een bestaand Bitdefender-abonnement dat op de account beschikbaar is, op voorwaarde dat ze voor hetzelfde product geldt.

Een abonnement activeren met een activatiecode:

1. Ga naar Bitdefender Central.
2. Ga naar het paneel **Mijn abonnementen**.
3. Klik op de knop **Activeringscode** en typ de code in het bijbehorende veld.
4. Klik op **Activeren** om door te gaan.

Het abonnement is nu geactiveerd. Ga naar het paneel **Mijn apparaten** en selecteer **BESCHERMING INSTALLEREN** om het product op een van uw apparaten te installeren.

6.4. Mijn apparaten

Vanaf het paneel **Mijn apparaten** van Bitdefender Central kunt u uw Bitdefender-product installeren, beheren en op afstand gebruiken op al uw apparaten die zijn ingeschakeld en verbinding hebben met internet. De apparaatkaarten geven de naam en de beveiligingsstatus van het apparaat

weer en geven weer of er beveiligingsrisico's zijn die de bescherming van uw apparaten beïnvloeden.

Klik op het uitklappijltje in de rechterbovenhoek van het scherm om de lijst van uw apparaten weer te geven naargelang hun status of hun gebruikers.

Om uw apparaten beter te kunnen herkennen, kunt u de apparaatnaam aanpassen:

1. Ga naar Bitdefender Central.
2. Selecteer het paneel **Mijn apparaten**.
3. Klik op de gewenste apparaatkaart en vervolgens op de icoon ⋮ in de rechterbovenhoek van het scherm.
4. Selecteer **Instellingen**.
5. Voer een nieuwe naam in het veld **Naam apparaat** in en klik op **OPSLAAN**.

Om het beheer van uw apparaten te vereenvoudigen, kunt u eigenaren instellen en aan de apparaten toewijzen:

1. Ga naar Bitdefender Central.
2. Selecteer het paneel **Mijn apparaten**.
3. Klik op de gewenste apparaatkaart en vervolgens op de icoon ⋮ in de rechterbovenhoek van het scherm.
4. Selecteer **Profiel**.
5. Klik op **Eigenaar toevoegen**, vul de bijbehorende velden in. Pas het profiel aan met de toevoeging van een foto en de instelling van een geboortedatum.
6. Klik op **Toevoegen** om het profiel op te slaan.
7. Selecteer de gewenste eigenaar uit de lijst **Apparaateigenaar** en klik op **Toewijzen**.

Bitdefender vanop afstand op een Windows-apparaat updaten:

1. Ga naar Bitdefender Central.
2. Selecteer het paneel **Mijn apparaten**.
3. Klik op de gewenste apparaatkaart en vervolgens op de icoon ⋮ in de rechterbovenhoek van het scherm.

4. Selecteer **Update**.

Voor meer acties van op afstand en informatie over uw Bitdefender-product op een specifiek toestel, klik op de gewenste toestelkaart.

Wanneer u op een apparaatkaart klikt, komen de volgende tabbladen beschikbaar:

- **Bedieningspaneel**. In dit venster vindt u gegevens over het geselecteerde apparaat, kunt u de beveiligingsstatus en de Bitdefender VPN-status nakijken en kunt u nagaan hoeveel bedreigingen de voorbije zeven dagen werden geblokkeerd. De beschermingsstatus kan groen zijn (dan zijn er geen problemen voor uw apparaat), geel (dan moet u het apparaat controleren) of rood (dan loopt uw apparaat een risico). Klik voor meer informatie op het uitklappijltje in het bovenste statusgebied indien uw apparaat problemen ondervindt. Van hieruit kunt u problemen manueel oplossen die de veiligheid van uw toestellen aantasten.
- **Bescherming**. Vanuit dit venster kunt u van op afstand een Snelle of Systeemscan uitvoeren op uw toestellen. Klik op de **SCAN**-knop om het proces te starten. U kunt ook nagaan wanneer de laatste scan werd uitgevoerd op het toestel en van de laatste scan met de belangrijkste informatie is er een verslag beschikbaar.Voor meer informatie over deze twee scanprocessen, verwijzen we naar Paragraaf 13.2.3, "*Een systeemscan uitvoeren*" en naar "*Een snelle scan uitvoeren*" (p. 80).
- **Kwetsbaarheid**. Om de eventuele kwetsbaarheid van een toestel te controleren, zoals ontbrekende Window-updates, verouderde applicaties of zwakke wachtwoorden, klik op de **SCAN**-knop in het tabblad Kwetsbaarheid. Kwetsbaarheden kunnen niet van op afstand afgehandeld worden. Indien er een kwetsbaarheid wordt opgemerkt, moet u een nieuwe scan op het toestel laten lopen en daarna de aanbevolen acties ondernemen. Klik op **Meer details** om naar een gedetailleerd rapport over de gevonden problemen te gaan. Zie "*Kwetsbaarheid*" (p. 101) voor meer informatie over deze functie.

6.5. Activiteit

In de Activiteitzone hebt u toegang tot informatie over de apparaten waar Bitdefender op geïnstalleerd is.

Wanneer u naar het **Activiteiten**-venster gaat, zijn de volgende kaarten beschikbaar:

- **Mijn apparaten**. Hier ziet u het aantal geconnecteerde apparaten, samen met hun beschermingsstatus. Om problemen voor de gedetecteerde apparaten vanop afstand op te lossen, klikt u op **Problemen oplossen** en vervolgens op **PROBLEMEN SCANNEN EN HERSTELLEN**.

  Om details te zien over de gedetecteerde problemen, klikt u op **Problemen bekijken**.

  Informatie over de gedetecteerde bedreigingen kan voor iOS-apparaten niet worden opgehaald.

- **Bedreigingen geblokkeerd**. Hier ziet u een grafiek met de algemene statistieken, met inbegrip van informatie over de bedreigingen die de voorbije 24 uur en 7 dagen werden geblokkeerd. De weergegeven informatie wordt opgehaald naargelang het schadelijke gedrag dat in de bestanden, toepassingen en url's werd gedetecteerd.
- **Topgebruikers met geblokkeerde bedreigingen**. Hier ziet u de gebruikers waarbij de meeste bedreigingen werden gevonden.
- **Topapparaten met geblokkeerde bedreigingen**. Hier ziet u de apparaten waarop de meeste bedreigingen werden gevonden.

6.6. Notificaties

Om u op de hoogte te houden van wat er gebeurt op de apparaten die aan uw account gekoppeld zijn, hebt u de 🔔-icoon ter beschikking. Zodra u erop klikt, krijgt u een algemeen beeld met informatie over de activiteit van de Bitdefender-producten die op uw apparaten geïnstalleerd zijn.

7. BITDEFENDER UP-TO-DATE HOUDEN

Elke dag worden er nieuwe bedreigingen gevonden en geïdentificeerd. Daarom is het heel belangrijk om Bitdefender up to date te houden met de nieuwste informatiedatabase voor bedreigingen.

Als u via breedband of DSL verbonden bent met het Internet, zal Bitdefender deze taak op zich nemen. Standaard controleert het of er updates zijn als u uw apparaat aanzet en ieder **uur** daarna. Als er een update beschikbaar is, wordt deze automatisch gedownload en op uw apparaat geïnstalleerd.

Het updateproces wordt geleidelijk uitgevoerd, wat betekent dat de te updaten bestanden een voor een worden vervangen. Hierdoor zal het updateproces de werking van het product niet beïnvloeden en wordt tegelijkertijd elk zwak punt uitgezonderd.

Belangrijk
Houd Automatische update ingeschakeld om u te beschermen tegen de laatste bedreigingen.

In sommige specifieke situaties is uw tussenkomst vereist om de bescherming van uw Bitdefender up-to-date te houden:

- Als uw apparaat een internetverbinding maakt via een proxyserver, moet u de proxy-instellingen configureren zoals beschreven in "*Bitdefender configureren voor het gebruik van een proxy-internetverbinding*" (p. 67).
- Als u met het Internet bent verbonden via een inbelverbinding, dan adviseren wij Bitdefender regelmatig handmatig te updaten. Zie "*Een update uitvoeren*" (p. 41) voor meer informatie.

7.1. Controleren of Bitdefender up-to-date is

Om te controleren wanneer de laatste update van uw Bitdefender plaatsvond:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Notificaties**.
2. In het tabblad **Alle** selecteert u de kennisgeving betreffende de recentste update.

U kunt uitzoeken wanneer updates werden gestart en u kunt informatie over de updates weergeven (of ze al dan niet gelukt zijn, of het opnieuw opstarten is vereist om de installatie te voltooien, enz.); Start, indien nodig, het systeem zo snel mogelijk opnieuw op.

7.2. Een update uitvoeren

Om updates uit te voeren is een internetverbinding vereist.

Klik op de Bitdefender B-icoon in het systeemvak en selecteer vervolgens **Nu updaten** om een update op te starten.

De functie Update maakt een verbinding met de updateserver van Bitdefender en controleert op updates. Als een update is gedetecteerd, wordt u gevraagd de update te bevestigen, of wordt de update automatisch uitgevoerd, afhankelijk van de Update-instellingen.

Belangrijk
Het kan noodzakelijk zijn de apparaat opnieuw op te starten wanneer de update is voltooid. Wij raden aan dit zo snel mogelijk te doen.

U kunt ook van op afstand updates uitvoeren op uw apparaten, op voorwaarde dat ze ingeschakeld zijn en met het internet verbonden zijn.

Bitdefender vanop afstand op een Windows-apparaat updaten:

1. Ga naar Bitdefender Central.
2. Selecteer het paneel **Mijn apparaten**.
3. Klik op de gewenste apparaatkaart en vervolgens op de icoon ⋮ in de rechterbovenhoek van het scherm.
4. Selecteer **Update**.

7.3. De automatische update in- of uitschakelen

De automatische update in- of uitschakelen:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Instellingen**.
2. Klik op het tabblad **Update**.
3. Schakel de overeenkomende schakelaar in of uit.
4. Er verschijnt een waarschuwingsvenster. U moet uw keuze bevestigen door in het menu te selecteren hoelang u de automatische update wilt uitschakelen. U kunt de automatische update uitschakelen gedurende 5, 15 of 30 minuten, 1 uur, of tot het systeem opnieuw wordt opgestart.

Waarschuwing
Dit is een kritiek beveiligingsprobleem. Wij raden u aan de automatische update zo kort mogelijk uit te schakelen. Als Bitdefender niet regelmatig wordt geüpdatet, zal het programma niet in staat zijn u te beschermen tegen de nieuwste bedreigingen.

7.4. De update-instellingen aanpassen

De updates kunnen worden uitgevoerd vanaf het lokale netwerk, via het Internet, rechtstreeks of via een proxyserver. Bitdefender zal standaard elk uur via het Internet controleren op updates en de beschikbare updates zonder enige waarschuwing installeren.

De standaardinstellingen voor de update zijn geschikt voor de meeste gebruikers en u hoeft ze normaal niet te wijzigen.

De update-instellingen aanpassen:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Instellingen**.
2. Selecteer het tabblad **Update** en pas de instellingen volgens uw voorkeuren aan.

Update-frequentie

Bitdefender is zo geconfigureerd dat het elk uur controleert op updates. Om de updatefrequentie te wijzigen, sleept u de glijder langs de schaal om de gewenste tijd in te stellen wanneer de update moet plaatsvinden.

Regels voor behandelen updates

Telkens wanneer er een update beschikbaar is, zal Bitdefender de update automatisch downloaden en invoeren zonder notificaties weer te geven. Schakel de optie **Stille update** uit indien u een notificatie wilt ontvangen telkens wanneer er een nieuwe update beschikbaar is.

Voor sommige updates moet het systeem opnieuw worden opgestart om de installatie te voltooien.

Als een update het opnieuw opstarten van het systeem vereist, blijft Bitdefender werken met de oude bestanden tot de gebruikers de apparaat opnieuw opstart. Hiermee wordt voorkomen dat de Bitdefender-update het werk van de gebruiker hinder.

Schakel **Opstartnotificatie** in als u verzocht wilt worden uw toestel terug op te starten wanneer een update dat vereist.

7.5. Doorlopende updates

Om zeker te zijn dat u de recentste versie gebruikt, controleert uw Bitdefender automatisch of er productupdates zijn. Deze updates kunnen nieuwe functies en verbeteringen hebben, productproblemen verhelpen of u een automatische upgrade naar een nieuwe versie bezorgen. Wanneer de nieuwe Bitdefender-versie via een update arriveert, worden persoonlijke instellingen opgeslagen en wordt de verwijderings- en herinstallatieprocedure overgeslagen.

Voor deze updates moet u het systeem opnieuw opstarten om de installatie van nieuwe bestanden te activeren. Nadat de productupdate voltooid is, verschijnt een popup-venster met de melding dat het systeem opnieuw moet worden opgestart. Indien u deze kennisgeving niet hebt gezien, kunt u ofwel klikken op **NU OPNIEUW OPSTARTEN** in het venster Kennisgevingen waar de recentste update wordt vermeld, of het systeem manueel opnieuw opstarten.

Opmerking

De updates met nieuwe functies en verbeteringen worden enkel aan gebruikers geleverd bij wie Bitdefender 2020 geïnstalleerd is.

ZO WERKT HET

8. INSTALLATIE

8.1. Hoe installeer ik Bitdefender op een tweede apparaat?

Indien de abonnement dat u hebt gekocht meer dan één apparaat dekt, kunt u uw Bitdefender-account gebruiken om een tweede pc te activeren.

Om Bitdefender te installeren op een tweede apparaat:

1. Klik op **Installeren op ander apparaat** in de linkerbenedenhoek van de Bitdefender-interface.

   Er verschijnt een nieuw venster op uw scherm.

2. Klik op **DOWNLOADLINK DELEN**.
3. Volg de aanwijzingen op het scherm om Bitdefender te installeren.

Het nieuwe toestel waarop u het Bitdefender-product hebt geïnstalleerd, zal op uw Bitdefender Central-bedieningspaneel verschijnen.

8.2. Hoe kan ik Bitdefender opnieuw installeren?

Typische situaties waarin u Bitdefender opnieuw moet installeren, zijn ondermeer de volgende:

- u hebt het besturingssysteem opnieuw geïnstalleerd..
- u wilt problemen oplossen die mogelijk voor vertragingen en crashes hebben gezorgd
- uw Bitdefender-product start of werkt niet naar behoren.

Indien een van de vermelde situaties op jou van toepassing is, volg dan deze stappen:

- In **Windows 7**:
  1. Klik op **Start** en ga naar **Alle Programma's**.
  2. **Bitdefender Antivirus Plus** vinden en **De-installeren** selecteren.
  3. Klik op **OPNIEUW INSTALLEREN** in het venster dat verschijnt.
  4. U moet de apparaat opnieuw opstarten om het proces te voltooien.
- In **Windows 8 en Windows 8.1**:

1. Zoek vanuit het Windows-startscherm het **Configuratiescherm** (u kunt bijvoorbeeld starten met het typen van "configuratiescherm", rechtstreeks in het startscherm) en klik op het pictogram ervan.
2. Klik op **Een programma verwijderen** of **Programma's en onderdelen**.
3. **Bitdefender Antivirus Plus** vinden en **De-installeren** selecteren.
4. Klik op **OPNIEUW INSTALLEREN** in het venster dat verschijnt.
5. U moet de apparaat opnieuw opstarten om het proces te voltooien.

- In **Windows 10**:

1. Klik op **Start**, klik dan op Instellingen.
2. Klik op de **Systeem**-icoon in Instellingen, selecteer dan **Apps & functies**.
3. **Bitdefender Antivirus Plus** vinden en **De-installeren** selecteren.
4. Klik nogmaals op **De-installeren** om uw keuze te bevestigen.
5. Klik op **OPNIEUW INSTALLEREN**.
6. U moet de apparaat opnieuw opstarten om het proces te voltooien.

Opmerking
Als u deze procedure voor opnieuw installeren volgt, worden persoonlijke instellingen opgeslagen, die in het nieuw geïnstalleerde product ook beschikbaar blijven. Andere instellingen kunnen teruggesteld worden naar hun fabriekskonfiguratie.

8.3. Waar kan ik mijn Bitdefender-product van downloaden?

U kunt Bitdefender installeren vanaf de installatiedisk of via de web installer die u naar uw computer kunt downloaden vanaf uw apparaat via het Bitdefender Central-platform.

Opmerking
Voordat u de kit uitvoert, raden we aan om beveiligingsoplossingen die op uw systeem zijn geïnstalleerd, te verwijderen. Wanneer u meer dan één beveiligingsoplossing op dezelfde apparaat gebruikt, wordt het systeem onstabiel.

Bitdefender installeren via Bitdefender Central:

1. Ga naar Bitdefender Central.
2. Selecteer het paneel **Mijn Apparaten** en klik dan op **BESCHERMING INSTALLEREN**.
3. Kies een van de twee beschikbare opties:

   - **Bescherm dit apparaat**

     Selecteer deze optie en selecteer dan de eigenaar van het apparaat. Als die apparaat aan iemand anders toebehoort, klik dan op de overeenstemmende knop.

   - **Bescherm andere apparaten**

     Selecteer deze optie en selecteer dan de eigenaar van het apparaat. Als die apparaat aan iemand anders toebehoort, klik dan op de overeenstemmende knop.

     Klik op **DOWNLOADLINK VERSTUREN**. Voer een e-mailadres in het overeenkomstige veld in en klik op **E-MAIL VERZENDEN**. De gegenereerde downloadlink is slechts 24 uur geldig. Indien de link vervalt, dient u aan de hand van dezelfde stappen een nieuwe te genereren.

     Controleer op het apparaat waarop u uw Bitdefender-product wilt installeren het e-mailadres dat u ingevoerd hebt en klik op de overeenkomstige downloadknop.
4. Start het gedownloade Bitdefender-programma.

8.4. Hoe kan ik de taal van mijn Bitdefender-product veranderen?

De interface van Bitdefender is beschikbaar in meerdere talen. U kunt de taal aan de hand van de volgende stappen aanpassen:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Instellingen**.
2. Klik in het venster **Algemeen** op **Taal wijzigen**.
3. Selecteer de gewenste taal uit de lijst en klik op **OPSLAAN**.
4. Wacht even tot de instellingen toegepast zijn.

8.5. Hoe gebruik ik mijn Bitdefender-abonnement na een Windows-upgrade?

Deze situatie doet zich voor wanneer u uw besturingssysteem upgrade en verder wilt gaan met het gebruik van uw Bitdefender-abonnement.

Als u een vorige versie van Bitdefender gebruikt, kunt u gratis upgraden naar de nieuwste Bitdefender op de volgende wijze:

- Van een vorige Bitdefender Antivirusversie naar de nieuwste Bitdefender Antivirus die beschikbaar is.
- Van een vorige Bitdefender Security for XP & Vista versie naar de nieuwste Bitdefender Security for XP & Vista die beschikbaar is.
- Van een vorige Bitdefender Total Security versie naar de nieuwste Bitdefender Total Security die beschikbaar is.

Er kunnen zich twee gevallen voordoen:

- U hebt het besturingssysteem bijgewerkt met gebruikmaking van Windows Update en u merkt dat Bitdefender niet langer werkt.

  Installeer het product in dit geval opnieuw door de volgende stappen te volgen:

  - In **Windows 7**:

    1. Klik op **Start**, ga naar **Configuratiescherm** en dubbelklik op **Programma's en onderdelen**.
    2. **Bitdefender Antivirus Plus** vinden en **De-installeren** selecteren.
    3. Klik op **OPNIEUW INSTALLEREN** in het venster dat verschijnt.
    4. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.

       Open de interface van uw nieuw geïnstalleerde Bitdefender-product om toegang te krijgen tot de functies ervan.

  - In **Windows 8 en Windows 8.1**:

    1. Zoek vanuit het Windows-startscherm het **Configuratiescherm** (u kunt bijvoorbeeld starten met het typen van "configuratiescherm", rechtstreeks in het startscherm) en klik op het pictogram ervan.
    2. Klik op **Een programma verwijderen** of **Programma's en onderdelen**.

3. **Bitdefender Antivirus Plus** vinden en **De-installeren** selecteren.
4. Klik op **OPNIEUW INSTALLEREN** in het venster dat verschijnt.
5. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.

   Open de interface van uw nieuw geïnstalleerde Bitdefender-product om toegang te krijgen tot de functies ervan.

- In **Windows 10**:

1. Klik op **Start**, klik dan op Instellingen.
2. Klik in Instellingen op de icoon **Systeem** en selecteer dan **Apps**..
3. **Bitdefender Antivirus Plus** vinden en **De-installeren** selecteren.
4. Klik nogmaals op **De-installeren** om uw keuze te bevestigen.
5. Klik op **OPNIEUW INSTALLEREN** in het venster dat verschijnt.
6. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.

   Open de interface van uw nieuw geïnstalleerde Bitdefender-product om toegang te krijgen tot de functies ervan.

> **Opmerking**
> Als u deze procedure voor opnieuw installeren volgt, worden persoonlijke instellingen opgeslagen, die in het nieuw geïnstalleerde product ook beschikbaar blijven. Andere instellingen kunnen teruggesteld worden naar hun fabriekskonfiguratie.

- U hebt uw systeem gewijzigd en u wilt doorgaan met het gebruik van de beveiliging van Bitdefender. Daarvoor moet u het product opnieuw installeren met gebruikmaking van de nieuwste versie.

  Om dit probleem op te lossen:

1. Download het installatiebestand:
   a. Ga naar Bitdefender Central.
   b. Selecteer het paneel **Mijn Apparaten** en klik dan op **BESCHERMING INSTALLEREN**.
   c. Kies een van de twee beschikbare opties:
      - **Bescherm dit apparaat**

Selecteer deze optie en selecteer dan de eigenaar van het apparaat. Als die apparaat aan iemand anders toebehoort, klik dan op de overeenstemmende knop.

- **Bescherm andere apparaten**

  Selecteer deze optie en selecteer dan de eigenaar van het apparaat. Als die apparaat aan iemand anders toebehoort, klik dan op de overeenstemmende knop.

  Klik op **DOWNLOADLINK VERSTUREN**. Voer een e-mailadres in het overeenkomstige veld in en klik op **E-MAIL VERZENDEN**. De gegenereerde downloadlink is slechts 24 uur geldig. Indien de link vervalt, dient u aan de hand van dezelfde stappen een nieuwe te genereren.

  Controleer op het apparaat waarop u uw Bitdefender-product wilt installeren het e-mailadres dat u ingevoerd hebt en klik op de overeenkomstige downloadknop.

2. Start het gedownloade Bitdefender-programma.

Raadpleeg "*Uw Bitdefender-product installeren*" (p. 5) voor meer informatie over het Bitdefender-installatieproces.

8.6. Hoe kan ik upgraden naar de recentste Bitdefender-versie?

Vanaf nu kunt u naar de nieuwste versie upgraden zonder de handmatige de-installatie- en installatie-procedures te volgen. Het nieuwe product, wordt meer bepaald samen met nieuwe functies en ingrijpende verbeteringen in het product, geleverd via productupdate en als u al een actieve Bitdefender-abonnement hebt, wordt het product automatisch geactiveerd.

Indien u de versie van 2020 gebruikt, kunt u naar de nieuwste versie upgraden aan de hand van de volgende stappen:

1. Klik op **NU OPNIEUW OPSTARTEN** in de kennisgeving die u ontvangt met de upgrade-informatie. Als u deze gemist hebt, ga naar het venster Kennisgevingen, ga naar de recentste update en klik vervolgens op de knop **NU OPNIEUW OPSTARTEN**. Wacht totdat het apparaat opnieuw is opgestart.

   Het venster **Wat is er nieuw** verschijnt, met informatie over de verbeterde en nieuwe functies.

2. Klik op de koppelingen **Meer weten** om doorgestuurd te worden naar de specifieke pagina, met meer informatie en nuttige artikels.
3. Sluit het venster **Wat is er nieuw** om naar de interface van de nieuw geïnstalleerde versie te gaan.

Gebruikers die gratis willen upgraden van Bitdefender 2016 of een lagere versie naar de nieuwste Bitdefender-versie moeten hun huidige versie verwijderen uit het controlepaneel en vervolgens het recentste installatiebestand downloaden via de Bitdefender-website op het volgende adres:http://www.bitdefender.nl/Downloads/. De activatie is enkel mogelijk met een geldig abonnement.

9. BITDEFENDER CENTRAL

9.1. Hoe meldt u zich met een andere account aan voor Bitdefender-account?

U hebt een nieuwe Bitdefender-account aangemaakt en u wilt deze van nu af aan gebruiken.

Om succesvol in te loggen met een andere Bitdefender-account:

1. Klik op uw accountnaam in het bovenste gedeelte van de Bitdefender-interface.
2. Klik in de rechterbovenhoek van het scherm op **Account wisselen** om de account gelinkt aan de apparaat te wisselen.
3. Voer het e-mailadres in het daarvoor bestemde veld en klik daarna op **VOLGENDE**.
4. Voer uw wachtwoord in en klik op **AANMELDEN**.

Opmerking
Het Bitdefender-product van uw toestel verandert automatisch volgens het abonnement dat verbonden is met de nieuwe Bitdefender-account.
Als er geen beschikbaar abonnement gekoppeld is aan de Bitdefender-account, of als u deze wilt overzetten naar de vorige account, kunt u contact opnemen met Bitdefender voor ondersteuning, zoals beschreven in deel "*Hulp vragen*" (p. 165).

9.2. Hoe schakel ik Bitdefender Central-hulpberichten uit?

Om u te helpen begrijpen waar elke optie in Bitdefender Central nuttig voor is, worden hulpberichten op de overzichtspagina weergegeven.

Indien u deze berichten niet meer wil zien:

1. Ga naar Bitdefender Central.
2. Klik bovenaan rechts op het scherm op de icoon .
3. Klik op **Mijn account** in het schuifmenu.
4. Klik op **Instellingen** in het schuifmenu.

5. Schakel de optie **Hulpberichten in/uitschakelen** uit.

9.3. Ik ben het wachtwoord dat ik voor mijn Bitdefender-account heb gekozen, vergeten. Hoe kan ik het terugstellen?

Er zijn twee mogelijkheden om een nieuw wachtwoord in te stellen voor uw Bitdefender-account:

- Vanuit de Bitdefender-interface:
  1. Klik in het navigatiemenu in de Bitdefender-interface op **Mijn account**.
  2. Klik in de rechterbovenhoek van het scherm op **Account wisselen**.

     Er verschijnt een nieuw venster.
  3. Voer uw e-mailadres in en klik op **VOLGENDE**.

     Er verschijnt een nieuw venster.
  4. Klik op **Wachtwoord vergeten?**.
  5. Klik op **VOLGENDE**.
  6. Controleer uw e-mailaccount, voer de beveiligingscode in die u ontvangen hebt en klik op **VOLGENDE**.

     Of u kunt in de e-mail die we naar u gestuurd hebben, klikken op **Wachtwoord wijzigen**.
  7. Geef het nieuwe wachtwoord dat u wilt instellen in en geef het vervolgens opnieuw in. Klik op **OPSLAAN**.
- Vanuit uw webbrowser:
  1. Ga naar https://central.bitdefender.com.
  2. Klik op **AANMELDEN**.
  3. Voer uw e-mailadres in en klik op **VOLGENDE**.
  4. Klik op **Wachtwoord vergeten?**.
  5. Klik op **VOLGENDE**.
  6. Controleer uw e-mailaccount en volg de instructies om een nieuw wachtwoord in te stellen voor uw Bitdefender-account.

Om naar uw Bitdefender-account te gaan tikt u voortaan uw e-mailadres en het wachtwoord in dat u net ingesteld hebt.

9.4. Hoe kan ik de aanmeldsessies van mijn Bitdefender-account beheren?

In uw Bitdefender-account kunt u de recentste inactieve en actieve aanmeldsessies op de apparaten van uw account bekijken. Bovendien kunt u van op afstand afmelden via deze stappen:

1. Ga naar Bitdefender Central.
2. Klik bovenaan rechts op het scherm op de icoon .
3. Klik op **Instellingen** in het schuifmenu.
4. In **Actieve sessies** selecteert u de optie **AFMELDEN** naast het apparaat waar u de aanmeldsessie wenst stop te zetten.

10. SCANNEN MET BITDEFENDER

10.1. Een bestand of map scannen

De eenvoudigste manier om een bestand of map te scannen is klikken met de rechtermuisknop op het object dat u wilt scannen, Bitdefender aanwijzen en **Scannen met Bitdefender** te selecteren in het menu.

Volg de Antivirusscanwizard om de scan te voltooien. Bitdefender zal automatisch de aanbevolen acties ondernemen op de gedetecteerde bestanden.

Als er niet opgeloste bedreigingen achterblijven, wordt u gevraagd de acties te kiezen die moeten worden ondernomen.

Typische situaties voor het gebruik van deze scanmethode zijn ondermeer de volgende:

- U vermoedt dat een specifiek bestand of een specifieke map geïnfecteerd is.
- Wanneer u bestanden waarvan u denkt dat ze mogelijk gevaarlijk zijn, downloadt van Internet.
- Scan een netwerkshare voordat u bestanden naar uw apparaat kopieert.

10.2. Hoe kan ik mijn systeem scannen?

Om een volledige scan van het systeem uit te voeren:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Bescherming**.
2. In het deelvenster **ANTIVIRUS** klikt u op **Openen**.
3. Klik op de knop **Scan uitvoeren** naast **Systeemscan**.
4. Volg de Systeemscanwizard om de scan te voltooien. Bitdefender zal automatisch de aanbevolen acties ondernemen op de gedetecteerde bestanden.

   Als er niet opgeloste bedreigingen achterblijven, wordt u gevraagd de acties te kiezen die moeten worden ondernomen. Zie "*Antivirusscanwizard*" (p. 84) voor meer informatie.

10.3. Hoe plan ik een scan?

U kunt uw Bitdefender-product instellen om belangrijke systeemlocaties te beginnen scannen wanneer u niet voor de apparaat zit.

Een scan plannen:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Bescherming**.
2. In het deelvenster **ANTIVIRUS** klikt u op **Openen**.
3. Klik in het onderste gedeelte van de interface op ••• naast het scantype dat u wilt inplannen, Systeemscan of Snelle scan, en selecteer vervolgens **Bewerken**.

   U kunt ook een scantype maken dat bij uw noden past, door te klikken op **+Scan maken** naast **Scans beheren**.
4. Pas de scan aan in overeenkomst met uw noden, en klik op **Volgende**.
5. Vink het vakje naast **Kiezen wanneer deze taak wordt ingepland** aan.

   Selecteer een van de overeenkomstige opties om een planning in te stellen:

   - Bij opstarten systeem
   - Dagelijks
   - Wekelijks
   - Maandelijks

   Kiest u Dagelijks, Maandelijks of Wekelijks, versleept u de schuifregelaar op de schaal om te kiezen wanneer de ingeplande scan moet starten.

Het venster **Scantaak** verschijnt als u ervoor kiest een nieuwe aangepaste scan aan te maken. Hier kunt u de locaties selecteren die u wilt laten scannen.

10.4. Een aangepaste scantaak maken

Als u specifieke locaties wilt scannen op uw apparaat of de scanopties wilt configureren, kunt u een aangepaste scantaak configureren en uitvoeren.

Ga als volgt te werk om een aangepaste scantaak te maken:

1. In het deelvenster **ANTIVIRUS** klikt u op **Openen**.
2. Klik naast **Scans beheren** op **+Scan maken**.

3. Voer in het veld Taaknaam een naam in voor de scan, selecteer vervolgens de locaties die u wilt laten scannen en klik op **VOLGENDE**.
4. Configureer deze algemene opties:
   - **Enkel toepassingen scannen**. U kunt Bitdefender zo instellen dat enkel toepassingen waartoe toegang wordt gezocht, worden gescand.
   - **Prioriteit scantaak**. U kunt kiezen welke impact een scanprocedure mag hebben op de prestaties van uw systeem.
     - Auto - De prioriteit van de scanprocedure hangt af van de systeemactiviteit. Om te verzekeren dat de scanprocedure geen invloed heeft op de systeemactiviteit, beslist Bitdefender of de scanprocedure met een hoge of lage prioriteit moet worden uitgevoerd.
     - Hoog - De prioriteit van de scanprocedure is hoog. Door deze optie te selecteren, laat u andere programma's trager werken, en verkort u de tijd die nodig is om de scanprocedure te voltooien.
     - Laag - De prioriteit van de scanprocedure is laag. Door deze optie te selecteren, laat u andere programma's sneller werken, en verlengt u de tijd die nodig is om de scanprocedure te voltooien.
   - **Acties na het scannen**. Kies welke actie Bitdefender moet ondernemen als er geen bedreigingen zijn gevonden:
     - Venster met samenvatting weergeven
     - Apparaat uitschakelen
     - Scanvenster sluiten
5. Als u de scanopties in detail wilt configureren, klikt u op **Geavanceerde opties weergeven**.

   Klik op **Volgende**.
6. U kunt de optie **Scantaak inplannen** inschakelen als u dat wenst. Vervolgens kiest u wanneer de aangepaste taak die u hebt gemaakt, moet worden gestart.
   - Bij opstarten systeem
   - Dagelijks
   - Maandelijks

- Wekelijks

  Kiest u Dagelijks, Maandelijks of Wekelijks, versleept u de schuifregelaar op de schaal om te kiezen wanneer de ingeplande scan moet starten.

7. Klik op **OPSLAAN** om de instellingen op te slaan en sluit het configuratievenster.

   Afhankelijk van de locaties die moeten worden gescand, kan het scannen even duren. Indien er tijdens de scanprocedure bedreigingen worden gevonden, wordt u gevraagd de acties te kiezen die in verband met de gedetecteerde bestanden moeten worden ondernomen.

Als u dat wenst, kunt u snel een eerdere aangepaste scan opnieuw uitvoeren door in de beschikbare lijst te klikken.

10.5. Hoe sluit ik een map uit van de scan?

Met Bitdefender kunt u specifieke bestanden, mappen of bestandsextensies uitsluiten van het scannen.

Uitsluitingen zijn bedoeld voor gebruikers met een gevorderde computerkennis en alleen in de volgende situaties:

- U hebt een grote map op uw systeem waarin u films en muziek bewaart.
- U hebt een groot archief op uw systeem waarin u verschillende gegevens bewaart.
- U bewaart een map waarin u verschillende types software en toepassingen installeert voor testdoeleinden. Het scannen van de map kan resulteren in het verlies van bepaalde gegevens.

Om een map toe te voegen aan de lijst Uitsluitingen:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Bescherming**.
2. In het deelvenster **ANTIVIRUS** klikt u op **Openen**.
3. Klik op het tabblad **Instellingen**.
4. Klik op **Uitzonderingen beheren**.
5. Klik op **+Een uitzondering toevoegen**.
6. Voer in het overeenkomende veld het pad in van de map die u wilt uitsluiten van het scannen.

U kunt ook naar de map navigeren door te klikken op de knop Bladeren aan de rechterkant van de interface. Selecteer de map en klik op **OK**.

7. Schakel de schakelaar naast de beschermingsvoorziening die de map niet moet scannen, in. Er zijn drie opties:
   - Antivirus
   - Preventie van online dreigingen
   - Advanced Threat Defense
8. Klik op **Opslaan** om de wijzigingen op te slaan en het venster te sluiten.

10.6. Wat moet ik doen wanneer Bitdefender een schoon bestand als geïnfecteerd beschouwt?

Er kunnen gevallen zijn waarbij Bitdefender een rechtmatig bestand verkeerdelijk markeert als een bedreiging (vals positief). Om deze fout te corrigeren, voegt u het bestand toe aan het gebied Uitsluitingen van Bitdefender:

1. Schakel de real time-antivirusbeveiliging van Bitdefender uit.
   a. Klik in het navigatiemenu in de Bitdefender-interface op **Bescherming**.
   b. In het deelvenster **ANTIVIRUS** klikt u op **Openen**.
   c. Schakel **Bitdefender Shield** uit in het venster **Shield**.

      Er verschijnt een waarschuwingsvenster. U moet uw keuze bevestigen door in het menu te selecteren hoelang u de real time-beveiliging wilt uitschakelen. U kunt de real time-beveiliging uitschakelen gedurende 5, 15 of 30 minuten, 1 uur, definitief of tot een systeem opnieuw wordt opgestart.
2. Verborgen objecten weergeven in Windows. Om te weten hoe u dit kunt doen, ga naar "*Verborgen objecten weergeven in Windows*" (p. 69).
3. Het bestand herstellen vanaf het quarantainegebied:
   a. Klik in het navigatiemenu in de Bitdefender-interface op **Bescherming**.
   b. In het deelvenster **ANTIVIRUS** klikt u op **Openen**.
   c. Ga naar de vensters **Instellingen** en klik op **Quarantaine beheren**.
   d. Selecteer het bestand en klik op **HERSTEL**.

4. Voeg het bestand toe aan de lijst Uitsluitingen. Om te weten hoe u dit kunt doen, ga naar "*Hoe sluit ik een map uit van de scan?*" (p. 58).

   Bitdefender is standaard zo ingesteld dat het herstelde bestanden automatisch toegevoegd aan de uitzonderingenlijst.

5. Schakel de real time antivirusbeveiliging van Bitdefender in.

6. Neem contact op met de medewerkers van onze ondersteuningsdienst zodat wij de detectie van de update van de bedreigingsinformatie kunnen verwijderen. Om te weten hoe u dit kunt doen, ga naar "*Hulp vragen*" (p. 165).

10.7. Hoe kan ik controleren welke bedreigingen Bitdefender heeft gedetecteerd?

Telkens wanneer een scan wordt uitgevoerd, wordt een scanlogboek gemaakt en registreert Bitdefender de verwijderde problemen.

Het scanlog bevat gedetailleerde informatie over het gevolgde scanproces, zoals de scanopties, het scandoel, de gevonden bedreigingen en de hierop uitgevoerde acties.

Zodra het scannen is voltooid, kunt u het scanlogboek direct vanaf de scanwizard openen door op **LOGBOEK WEERGEVEN** te klikken.

Een scanlog of een gedetecteerde infectie later bekijken:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Notificaties**.
2. In het tabblad **Alle** selecteert u de kennisgeving betreffende de recentste scan.

   Hier vindt u alle gebeurtenissen van scans op bedreigingen, inclusief bedreigingen die zijn gedetecteerd door Scannen bij toegang, door gebruiker gestarte scans en statuswijzigingen voor automatische scans.
3. In de kennisgevingenlijst kunt u controleren welke scans onlangs werden uitgevoerd. Klik op een kennisgeving om details erover weer te geven.
4. Klik op **Logboek weergeven** om het scanlogboek te openen.

11. PRIVACY BESCHERMING

11.1. Hoe kan ik controleren of mij online transactie beveiligd is?

Als u wilt controleren of uw online bewerkingen privé blijven, kunt u de browser die door Bitdefender is geleverd, gebruiken voor het beschermen van uw transacties en toepassingen voor thuisbankieren.

Bitdefender Safepay™ is een beveiligde browser die is ontwikkeld om uw creditcardgegevens, accountnummer of andere vertrouwelijke gegevens die u mogelijk invoert bij toegang tot verschillende online locaties, te beschermen.

Uw online activiteit veilig en privé houden:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Privacy**.
2. Klik op **Instellingen** in het deelvenster **SAFEPAY**.
3. In de vensters **Safepay** klikt u op **Safepay starten**.
4. Klik op de knop om toegang te krijgen tot het **virtuele toetsenbord**.

   Gebruik het **virtuele toetsenbord** wanneer u vertrouwelijke informatie, zoals uw wachtwoorden, invoert.

11.2. Hoe kan ik een bestand definitief verwijderen met Bitdefender?

Als u een bestand definitief van uw systeem wilt verwijderen, moet u de gegevens fysiek verwijderen van uw harde schijf.

De Bestandsvernietiging van Bitdefender helpt u aan de hand van de onderstaande stappen bestanden of mappen snel te vernietigen via het contextmenu van Windows:

1. Klik met de rechtermuisknop op het bestand of de map die u definitief wilt verwijderen, wijs Bitdefender aan en selecteer **Bestandsvernietiging**.
2. Klik op **PERMANENT VERWIJDEREN** en bevestig dat u het proces wilt voortzetten.

   Wacht tot Bitdefender het vernietigen van de bestanden heeft voltooid.

3. De resultaten worden weergegeven. Klik op **BEËINDIGEN** om de wizard te verlaten.

11.3. Hoe kan ik versleutelde bestanden handmatig herstellen wanneer het herstelproces faalt?

Indien de versleutelde bestanden niet automatisch worden hersteld, kunt u ze handmatig herstellen aan de hand van de volgende stappen:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Notificaties**.
2. In het tabblad **Alle** selecteert u de notificatie betreffende het ransomware-gedrag dat als laatste werd gedetecteerd en klikt u op **Versleutelde bestanden**.
3. De lijst met versleutelde bestanden wordt weergegeven.

   Klik op **BESTANDEN HERSTELLEN** om verder te gaan.
4. Indien een deel van of het gehele herstelproces mislukt, moet u de locatie kiezen waar de ontcijferde bestanden moeten worden bewaard. Klik op **LOCATIE VOOR HET HERSTEL** en kies een locatie op uw pc.
5. Er wordt een bevestigingsvenster weergegeven.

   Klik op **VOLTOOIEN** om het herstelproces te beëindigen.

Bestanden met de onderstaande extensies kunnen worden hersteld, indien ze worden versleuteld:

.3g2; .3gp; .7z; .ai; .aif; .arj; .asp; .aspx; .avi; .bat; .bin; .bmp; .c; .cda; .cgi; .class; .com; .cpp; .cs; .css; .csv; .dat; .db; .dbf; .deb;.doc; .docx; .gif; .gz; .h264; .h; .flv; .htm; .html;.ico; .jar; .java; .jpeg; .jpg;.js; .jsp; .key; .m4v; .mdb; .mid; .midi; .mkv; .mp3; .mp4; .mov; .mpg; .mpeg; .ods; .odp;.odt; .ogg; .pdf; .pkg; .php; .pl; .png; .pps; .ppt; .pptx; .ps; .psd; .py; .rar; .rm; .rtf; .sav; .sql; .sh; .svg; .swift; .swf; .tar; .tex; .tif; .tiff; .txt; .xlr; .xls; .xlsx; .xml; .wmv; .vb; .vob; .wav; .wks; .wma; .wpl; .wps; .wpd; .wsf; .z; .zip;

12. NUTTIGE INFORMATIE

12.1. Hoe test ik mijn beveiligingsoplossing?

Om er zeker van te zijn dat uw Bitdefender-product correct werkt, raden we u aan de Eicartest te gebruiken.

Met de Eicartest kunt u uw beveiligingsoplossing controleren met een veilig bestand dat hiervoor is ontwikkeld.

Om uw beveiligingsoplossing te testen:

1. Download de test van de officiële webpagina van de EICAR-organisatie http://www.eicar.org/.
2. Klik op de tab **Antimalware Testbestand**.
3. Klik in het menu aan de linkerzijde op **Downloaden**.
4. Vanuit **Downloadgedeelte met gebruikmaking van standaardprotocol http** klikt u op het testbestand **eicar.com**.
5. U zult worden geïnformeerd dat de pagina die u probeert te bezoeken het EICAR-Testbestand bevat (geen bedreiging).

   Indien u klikt op **Ik begrijp de risico's, breng me er toch heen**, dat start de download van de test en een Bitdefender-pop-up informeert u dat er een bedreiging is gedetecteerd.

   Klik op **Meer details** om meer informatie over deze handeling te krijgen.

Indien u geen Bitdefender-waarschuwing wilt ontvangen, raden we u aan om contact op te nemen met Bitdefender voor ondersteuning zoals beschreven in deel "*Hulp vragen*" (p. 165).

12.2. Hoe kan ik Bitdefender verwijderen?

Als u uw Bitdefender Antivirus Plus wilt verwijderen:

- In **Windows 7**:
  1. Klik op **Start**, ga naar **Configuratiescherm** en dubbelklik op **Programma's en onderdelen**.
  2. **Bitdefender Antivirus Plus** vinden en **De-installeren** selecteren.
  3. Klik op **VERWIJDEREN** in het venster dat verschijnt.

4. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.

- In **Windows 8 en Windows 8.1**:

  1. Zoek vanuit het Windows-startscherm het **Configuratiescherm** (u kunt bijvoorbeeld starten met het typen van "configuratiescherm", rechtstreeks in het startscherm) en klik op het pictogram ervan.
  2. Klik op **Een programma verwijderen** of **Programma's en onderdelen**.
  3. **Bitdefender Antivirus Plus** vinden en **De-installeren** selecteren.
  4. Klik op **VERWIJDEREN** in het venster dat verschijnt.
  5. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.

- In **Windows 10**:

  1. Klik op **Start**, klik dan op Instellingen.
  2. Klik in Instellingen op de icoon **Systeem** en selecteer dan **Apps**..
  3. **Bitdefender Antivirus Plus** vinden en **De-installeren** selecteren.
  4. Klik nogmaals op **De-installeren** om uw keuze te bevestigen.
  5. Klik op **VERWIJDEREN** in het venster dat verschijnt.
  6. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.

Opmerking
Deze procedure voor opnieuw installeren verwijdert uw persoonlijke instellingen permanent.

12.3. Hoe kan ik Bitdefender VPN verwijderen?

De procedure om Bitdefender VPN te verwijderen, is vergelijkbaar met de procedure om andere programma's van uw apparaat te verwijderen:

- In **Windows 7**:

  1. Klik op **Start**, ga naar **Configuratiescherm** en dubbelklik op **Programma's en onderdelen**.
  2. Zoek **Bitdefender VPN** en selecteer **Verwijderen**.

     Wacht tot de de-installatieproces is voltooid.

- In **Windows 8 en Windows 8.1**:
  1. Zoek vanuit het Windows-startscherm het **Configuratiescherm** (u kunt bijvoorbeeld starten met het typen van "configuratiescherm", rechtstreeks in het startscherm) en klik op het pictogram ervan.
  2. Klik op **Een programma verwijderen** of **Programma's en onderdelen**.
  3. Zoek **Bitdefender VPN** en selecteer **Verwijderen**.

     Wacht tot de de-installatieproces is voltooid.
- In **Windows 10**:
  1. Klik op **Start**, klik dan op Instellingen.
  2. Klik op het pictogram **Systeem** in Instellingen, selecteer dan **Geïnstalleerde apps**.
  3. Zoek **Bitdefender VPN** en selecteer **Verwijderen**.
  4. Klik nogmaals op **De-installeren** om uw keuze te bevestigen.

     Wacht tot de de-installatieproces is voltooid.

12.4. Hoe verwijder ik de extensie Anti-tracker van Bitdefender?

Afhankelijk van de webbrowser die u gebruikt, volgt u deze stappen om de extensie Anti-tracker van Bitdefender te de-installeren:

- Internet Explorer
  1. Klik op  naast de zoekbalk en selecteer Uitbreidingen beheren.

     Er verschijnt een lijst van de geïnstalleerde extensies.
  2. Klik op Anti-tracker van Bitdefender.
  3. Klik rechtsonder op **Uitschakelen**.
- Google Chrome
  1. Klik op naast de zoekbalk.
  2. Selecteer **Meer extra** en vervolgens **Extensies**.

     Er verschijnt een lijst van de geïnstalleerde extensies.
  3. Klik op **Verwijderen** in de kaart Anti-tracker van Bitdefender.

4. Klik op **Verwijderen** in de pop-up die verschijnt.

- Mozilla Firefox

1. Klik op  naast de zoekbalk.
2. Selecteer **Uitbreidingen** en vervolgens **Extensies**.

   Er verschijnt een lijst van de geïnstalleerde extensies.

3. Klik op ••• en selecteer vervolgens **Verwijderen**.

12.5. Hoe kan ik de apparaat automatisch afsluiten nadat het scannen is voltooid?

Bitdefender biedt meerdere scantaken die u kunt gebruiken om zeker te zijn dat uw systeem niet is geïnfecteerd door bedreigingen. Het scannen van de volledige apparaat kan langer duren, afhankelijk van de hardware- en softwareconfiguratie van uw systeem.

Omwille van deze reden biedt Bitdefender u de mogelijkheid om uw product te configureren om uw systeem af te sluiten zodra het scannen is voltooid.

Overweeg dit voorbeeld: u bent klaar met uw werk en wilt naar bed. U wilt dat Bitdefender uw volledig systeem controleert op bedreigingen.

Om de apparaat uit te schakelen wanneer Snelle scan of Systeemscan zijn voltooid:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Bescherming**.
2. In het deelvenster **ANTIVIRUS** klikt u op **Openen**.
3. In het venster **Scans** klikt u op ••• naast Snelle scan of Systeemscan en selecteert u **Bewerken**.
4. Pas de scan aan in overeenkomst met uw noden en klik op **Volgende**.
5. Vink het vakje naast **Kiezen wanneer deze taak wordt ingepland** aan en kies vervolgens wanneer de taak moet worden gestart.

   Kiest u Dagelijks, Maandelijks of Wekelijks, versleept u de schuifregelaar op de schaal om te kiezen wanneer de ingeplande scan moet starten.
6. Klik op **Opslaan**.

Om het apparaat uit te schakelen wanneer een aangepaste scan is voltooid:

1. Klik op ••• naast de aangepaste scan die u hebt aangemaakt.
2. Klik op **Volgende** en opnieuw op **Volgende**.
3. Vink het vakje naast **Kiezen wanneer deze taak wordt ingepland** aan en kies vervolgens wanneer de taak moet worden gestart.
4. Klik op **Opslaan**.

Als er geen bedreigingen zijn gevonden, wordt de apparaat uitgeschakeld.

Als er niet opgeloste bedreigingen achterblijven, wordt u gevraagd de acties te kiezen die moeten worden ondernomen. Zie "*Antivirusscanwizard*" (p. 84) voor meer informatie.

12.6. Bitdefender configureren voor het gebruik van een proxy-internetverbinding

Als uw apparaat een internetverbinding maakt via een proxyserver, moet u Bitdefender configureren met de proxy-instellingen. Bitdefender zal standaard de proxy-instellingen van uw systeem automatisch detecteren en importeren.

> **!** **Belangrijk**
> Internetverbindingen bij u thuis gebruiken doorgaans geen proxyserver. Als vuistregel is het aanbevolen de proxyverbindingsinstellingen van uw Bitdefender-programma te controleren en te configureren wanneer de updates niet werken. Als Bitdefender een update kan uitvoeren, dan is de toepassing correct geconfigureerd voor het maken van een internetverbinding.

Uw proxy-instellingen beheren:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Instellingen**.
2. Klik op het tabblad **Geavanceerd**.
3. Schakel **Proxyserver** in.
4. Klik op **Proxywijziging**.
5. Er zijn twee opties voor het instellen van de proxy-instellingen:
   - **Proxy-instellingen van de standaardbrowser importeren** - proxy-instellingen van de huidige gebruiker, opgehaald van de standaardbrowser. Als de proxyserver een gebruikersnaam en

wachtwoord vereist, moet u deze gegevens opgeven in de overeenkomende velden.

> **Opmerking**
> Bitdefender kan proxy-instellingen van de populairste browsers importeren, inclusief de nieuwste versies van Microsoft Edge, Internet Explorer, Mozilla Firefox en Google Chrome.

- **Proxy-instellingen aanpassen** - proxy-instellingen die u zelf kunt configureren. U moet de volgende instellingen definiëren:
  - **Adres** - voer het IP-adres van de proxyserver in.
  - **Poort** - voer de poort in die Bitdefender gebruikt om een verbinding te maken met de proxyserver.
  - **Gebruikersnaam** - voer een gebruikersnaam in die wordt herkend door de proxy.
  - **Wachtwoord** - voer het geldige wachtwoord voor de eerder opgegeven gebruiker in.

6. Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten.

Bitdefender gebruikt de beschikbare proxy-instellingen tot er een internetverbinding kan worden gemaakt.

12.7. Gebruik ik een 32- of 64-bits versie van Windows?

Nagaan of u een besturingssysteem van 32 bits of 64 bits hebt:

- In **Windows 7**:
  1. Klik op **Start**.
  2. Zoek **Computer** in het menu **Start**.
  3. Klik met de rechtermuisknop op **Deze computer** en selecteer **Eigenschappen**.
  4. Kijk onder **Systeem** om de informatie over uw systeem te controleren.
- In **Windows 8**:
  1. Zoek vanuit het Windows-startscherm **Computer** (u kunt bijvoorbeeld starten met het typen van "computer", rechtstreeks in het startscherm) en rechterklik op het pictogram ervan.

     Zoek in **Windows 8.1**, naar **Deze computer**.

2. Selecteer **Eigenschappen** in het onderste menu.
3. Kijk in Systeem om uw systeemtype te zien.

- In **Windows 10**:
  1. Typ "Systeem" in het zoekveld in de taakbalk en klik op het pictogram ervan.
  2. Kijk bij Systeem om informatie over uw systeemtype te vinden.

12.8. Verborgen objecten weergeven in Windows

Deze stappen zijn nuttig in de gevallen waarin u te maken krijgt met een bedreiging en u de geïnfecteerde bestanden die kunnen verborgen zijn, moet vinden en verwijderen.

Volg deze stappen om verborgen objecten weer te geven in Windows.

1. Klik op **Start**, ga naar **Beheerpaneel**.

   In **Windows 8 en Windows 8.1**: Zoek vanuit het Windows-startscherm het **Configuratiescherm** (u kunt bijvoorbeeld starten met het typen van "configuratiescherm", rechtstreeks in het startscherm) en klik op het pictogram ervan.
2. Selecteer **Mapopties**.
3. Ga naar het tabblad **Weergave**.
4. Selecteer **Verborgen bestanden en mappen weergeven**.
5. Vink **Extensies voor bekende bestandstypen verbergen** uit.
6. Schakel het selectievakje **Beveiligde besturingssysteembestanden verbergen** in.
7. Klik op **Toepassen**, klik daarna op **OK**.

In **Windows 10**:

1. Typ "Verborgen bestanden en mappen tonen" in het zoekveld in de taakbalk en klik op het pictogram ervan.
2. Selecteer **Verborgen bestanden, mappen en drives tonen**.
3. Vink **Extensies voor bekende bestandstypen verbergen** uit.
4. Schakel het selectievakje **Beveiligde besturingssysteembestanden verbergen** in.

5. Klik op **Toepassen**, klik daarna op **OK**.

12.9. Andere beveiligingsoplossingen verwijderen

De hoofdreden voor het gebruik van een beveiligingsoplossing is het bieden van bescherming en veiligheid voor uw gegevens. Maar wat gebeurt er als er meerdere beveiligingsproducten aanwezig zijn op hetzelfde systeem?

Wanneer u meer dan één beveiligingsoplossing op dezelfde apparaat gebruikt, wordt het systeem onstabiel. Het installatieprogramma van Bitdefender Antivirus Plus detecteert automatisch andere beveiligingsprogramma's en biedt u de mogelijkheid om ze te verwijderen.

Indien u de andere beveiligingsoplossingen niet hebt verwijderd tijdens de eerste installatie:

- In **Windows 7**:
  1. Klik op **Start**, ga naar **Configuratiescherm** en dubbelklik op **Programma's en onderdelen**.
  2. Wacht enkele ogenblikken tot de lijst met geïnstalleerde software wordt weergegeven.
  3. Zoek de naam van het programma dat u wilt verwijderen en selecteer **Verwijderen**.
  4. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.
- In **Windows 8 en Windows 8.1**:
  1. Zoek vanuit het Windows-startscherm het **Configuratiescherm** (u kunt bijvoorbeeld starten met het typen van "configuratiescherm", rechtstreeks in het startscherm) en klik op het pictogram ervan.
  2. Klik op **Een programma verwijderen** of **Programma's en onderdelen**.
  3. Wacht enkele ogenblikken tot de lijst met geïnstalleerde software wordt weergegeven.
  4. Zoek de naam van het programma dat u wilt verwijderen en selecteer **Verwijderen**.
  5. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.
- In **Windows 10**:

1. Klik op **Start**, klik dan op Instellingen.
2. Klik in Instellingen op de icoon **Systeem** en selecteer dan **Apps**..
3. Zoek de naam van het programma dat u wilt verwijderen en selecteer **Verwijderen**.
4. Klik nogmaals op **De-installeren** om uw keuze te bevestigen.
5. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.

Als u de andere beveiligingsoplossing niet van uw systeem kunt verwijderen, kunt u het hulpprogramma voor het verwijderen ophalen van de website van de verkoper of direct met hem contact opnemen voor richtlijnen betreffende het verwijderen.

12.10. Opnieuw opstarten in Veilige modus

De Veilige modus is een diagnostische gebruiksmodus die hoofdzakelijk wordt gebruikt om problemen op te lossen die de normale werking van Windows beïnvloeden. Dergelijke problemen kunnen lopen van conflicterende stuurprogramma's tot bedreigingen die verhinderen dat Windows normaal wordt gestart. In de Veilige modus werken slechts enkele toepassingen en laadt Windows alleen de basisbesturingsprogramma's en een minimum aan componenten van het besturingssysteem. Daarom zijn de meeste bedreigingen inactief wanneer Windows in de Veilige modus wordt gebruikt en kunnen ze gemakkelijk worden verwijderd.

Windows in Veilige modus starten:

- In **Windows 7**:
  1. Start uw apparaat opnieuw op.
  2. Druk meerdere keren op de **F8**-toets voordat Windows wordt gestart om toegang te krijgen tot het opstartmenu.
  3. Selecteer **Veilige modus** in het opstartmenu of **Veilige modus met netwerkmogelijkheden** als u internettoegang wenst.
  4. Druk op **Enter** en wacht terwijl Windows wordt geladen in Veilige modus.
  5. Dit proces eindigt met een bevestigingsbericht. Klik op **OK** om te bevestigen.
  6. Om Windows normaal te starten, hoeft u alleen het systeem opnieuw op te starten.

- In **Windows 8, Windows 8.1 en Windows 10**:

  1. Lanceer **Systeemconfiguratie** in Windows door tegelijk op de toetsen **Windows + R** op uw keyboard te drukken.
  2. Schrijf **msconfig** in het dialoogvenster **Openen** en klik daarna op **OK**.
  3. Selecteer het tabblad **Opstarten**.
  4. In het gebied **Opstartopties** vinkt u het vakje **Veilig opstarten** aan.
  5. Klik op **Netwerk** en vervolgens op **OK**.
  6. Klik op **OK** in het venster **Systeemconfiguratie** dat u vertelt dat het systeem opnieuw moet worden opgestart om de wijzigingen die u hebt ingesteld, door te voeren.

     Uw systeem wordt opnieuw opgestart in Veilige modus met Netwerk.

  Om opnieuw op te starten normale modus, zet u de instellingen terug door de **Systeemoperati** opnieuw te lanceren en het vakje **Veilig opstarten** terug uit te vinken. Klik op **OK** en daarna op **Opnieuw opstarten**. Wacht tot de nieuwe instellingen toegepast zijn.

UW BEVEILIGING BEHEREN

13. ANTIVIRUSBEVEILIGING

Bitdefender beveiligt uw apparaat tegen alle types bedreigingen (malware, Trojanen, spyware, rootkits enz.). De Bitdefender-bescherming is ingedeeld in twee categorieën:

- Scannen bij toegang - verhindert dat nieuwe bedreigingen uw systeem binnenkomen. Bitdefender zal bijvoorbeeld een Worddocument scannen op bekende gevaren wanneer u het opent, en een e-mailbericht wanneer u het ontvangt.

  Met Scannen bij toegang bent u zeker van bescherming in real time tegen bedreigingen, een essentieel onderdeel van elk computerbeveiligingsprogramma.

  Belangrijk
  Houd **Scannen bij toegang** ingeschakeld om te verhinderen dat bedreigingen uw apparaat infecteren.

- Scannen op aanvraag - hiermee kunt u de bedreiging die al op uw systeem aanwezig is, detecteren en verwijderen. Dit is de klassieke scan die door de gebruiker wordt geactiveerd. U selecteert het station, de map of het bestand dat Bitdefender moet scannen, en Bitdefender doet dat - op aanvraag.

Bitdefender scant automatisch alle verwisselbare media die op de apparaat zijn aangesloten om zeker te zijn dat ze veilig kunnen worden geopend. Zie "*Automatisch scannen van verwisselbare media*" (p. 88) voor meer informatie.

Geavanceerde gebruikers kunnen scanuitzonderingen configureren als ze niet willen dat specifieke bestanden of bestandstypes worden gescand. Zie "*Scanuitsluitingen configureren*" (p. 91) voor meer informatie.

Wanneer een bedreiging wordt gedetecteerd, zal Bitdefender automatisch proberen de kwaadwillige code uit het geïnfecteerde bestand te verwijderen en het originele bestand te reconstrueren. Deze bewerking wordt 'desinfecteren' genoemd. Bestanden die niet kunnen worden gedesinfecteerd, worden naar quarantaine verplaatst om de infectie in te dammen. Zie "*Bestanden in quarantaine beheren*" (p. 93) voor meer informatie.

Als uw apparaat werd geïnfecteerd door bedreigingen, moet u "*Bedreigingen van uw systeem verwijderen*" (p. 157) raadplegen. Om u te helpen bij het opruimen van de bedreigingen die niet kan worden verwijderd van het

Windows-besturingssysteem op uw apparaat, biedt Bitdefender u de "*Noodomgeving*" (p. 157). Dit is een vertrouwde omgeving, vooral ontworpen voor het verwijderen van bedreigingen, waarmee u uw apparaat onafhankelijk van Windows kunt opstarten. Wanneer het apparaat in de Noodomgeving wordt gebruikt, zijn Windows-dreigingen niet actief, waardoor het makkelijker is om ze te verwijderen.

13.1. Scannen bij toegang (real time-beveiliging)

Bitdefender biedt realtime bescherming tegen een breed gamma bedreigingen door alle bestanden en e-mailberichten waar toegang toe wordt gezocht, te scannen.

13.1.1. De real time-beveiliging in- of uitschakelen

De bescherming tegen bedreigingen in reële tijd in- of uitschakelen:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Bescherming**.
2. In het deelvenster **ANTIVIRUS** klikt u op **Openen**.
3. In het venster **Shield** schakelt u **Bitdefender Shield** in of uit.
4. Indien u bescherming in reële tijd wenst uit te schakelen, verschijnt een waarschuwingsscherm. U moet uw keuze bevestigen door in het menu te selecteren hoelang u de real time-beveiliging wilt uitschakelen. U kunt de real time-beveiliging uitschakelen gedurende 5, 15 of 30 minuten, 1 uur, definitief of tot een systeem opnieuw wordt opgestart. De realtime beveiliging wordt automatisch ingeschakeld als de geselecteerde tijd verloopt.

Waarschuwing
Dit is een kritiek beveiligingsprobleem. Wij raden u aan de real time-beveiliging zo kort mogelijk uit te schakelen. Als de real time-beveiliging is uitgeschakeld, wordt u niet beveiligd tegen bedreigingen.

13.1.2. De geavanceerde instellingen voor de realtime beveiliging configureren

Gevorderde gebruikers willen wellicht voordeel halen uit de scaninstellingen die door Bitdefender worden aangeboden. U kunt de instellingen voor de real

time-beveiliging in detail configureren door een aangepast beschermingsniveau te maken.

Om degeavanceerde instellingen voor de realtime beveiliging te configureren:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Bescherming**.
2. In het deelvenster **ANTIVIRUS** klikt u op **Openen**.
3. In het venster **Geavanceerd** kunt u de scaninstellingen configureren.

Informatie over de scanopties

Deze informatie kan nuttig zijn:

- **Enkel toepassingen scannen.** U kunt Bitdefender zo instellen dat enkel toepassingen waartoe toegang wordt gezocht, worden gescand.
- **Mogelijk ongewenste toepassingen scannen.** Selecteer deze optie om te scannen op ongewenste toepassingen. Een PUA (potentially unwanted application) of PUP (potentially unwanted program) is software die meestal wordt samengebundeld met freeware software en pop-ups weergeeft of een werkbalk in de standaardbrowser installeert. Sommige PUA's of PUP's veranderen de homepage of zoekmotor, anderen voeren op de achtergrond meerdere processen uit waardoor uw pc vertraagt of laten talrijke advertenties zien. Deze programma's kunnen zonder uw toestemming worden geïnstalleerd (ook wel adware genoemd) of worden standaard toegevoegd aan de uitdrukkelijke installatiekit (advertentie-ondersteund).
- **Scripts scannen.** Met de functie Scripts scannen kan Bitdefender powershellscripts en office-documenten scannen die scriptgebaseerde malware zou kunnen bevatten.
- **Gedeelde netwerken scannen.** Om een extern netwerk vanaf uw apparaat veilig te gebruiken, raden we aan dat u de optie Gedeelde netwerken scannen ingeschakeld laat.
- **Archieven scannen.** Het scannen binnenin de archieven verloopt langzaam en is een veeleisend proces, waardoor het niet aanbevolen is voor de realtime-beveiliging. Archieven die geïnfecteerde bestanden bevatten, zijn geen onmiddellijke bedreiging voor de beveiliging van uw systeem. De bedreiging kan uw systeem alleen beïnvloeden als het geïnfecteerde bestand wordt uitgepakt uit het archief en uitgevoerd zonder dat de real time-beveiliging is ingeschakeld.

Beslist u om deze optie te gebruiken, schakel deze dan in en versleep de schuifregelaar langs de schaal om archieven die groter zijn dan een bepaalde waarde in MB (Megabytes) uit te sluiten.

- **Opstartsectoren scannen.** U kunt Bitdefender instellen om de startgebieden van uw harde schijf te scannen. Dit deel van de harde schijf bevat de vereiste computercode om het opstartproces te starten. Als een bedreiging het opstartgebied besmet, kan de toegang tot de schijf geblokkeerd worden en het is mogelijk dat u dan uw systeem niet meer kunt starten en geen toegang meer hebt tot uw gegevens.
- **Enkel nieuwe en gewijzigde bestanden scannen.** Door alleen nieuwe en gewijzigde bestanden te scannen, kunt u de algemene reactiviteit van uw systeem aanzienlijk verbeteren met een minimale inlevering op het vlak van beveiliging.
- **Keyloggers scannen.** Selecteer deze optie om uw systeem te scannen op keyloggers. Keyloggers slaan op wat u op uw toetsenbord intypt en zenden via Internet verslagen naar een kwaadwillend persoon (hacker). De hacker kan gevoelige informatie uit de gestolen data halen, zoals bankrekeningnummers en wachtwoorden, en deze voor zijn eigen doeleinden gebruiken.
- **Vroege opstartscan.** Selecteer de optie **Vroege opstartscan** om uw systeem te scannen bij het opstarten, zodra alle kritieke diensten geladen zijn. De bedoeling van deze functie is om de detectie van bedreigingen bij de opstart van het systeem te verbeteren en de opstarttijd van uw systeem te verkorten.

Acties die worden ondernomen op gedetecteerde bedreigingen

U kunt de acties die door de realtime bescherming worden genomen configureren aan de hand van de volgende stappen:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Bescherming**.
2. In het deelvenster **ANTIVIRUS** klikt u op **Openen**.
3. In het venster **Geavanceerd** scrolt u naar beneden tot u de optie **Dreigingsacties** ziet.
4. Configureer de scaninstellingen zoals dat nodig is.

De volgende acties kunnen worden ondernomen door de realtime beveiliging in Bitdefender:

Neem gepaste acties

Bitdefender zal de aanbevolen acties ondernemen op basis van het type van het gedetecteerde bestand:

- **Geïnfecteerde bestanden.** Bestanden die als besmet zijn gedetecteerd, komen overeen met een stukje bedreigingsinformatie gevonden in de informatiedatabase voor bedreigingen van Bitdefender. Bitdefender zal automatisch proberen de kwaadaardige code van een geïnfecteerd bestand te verwijderen en het originele bestand te reconstrueren. Deze bewerking wordt 'desinfecteren' genoemd.

  Bestanden die niet kunnen worden gedesinfecteerd, worden naar quarantaine verplaatst om de infectie in te dammen. In quarantaine geplaatst bestanden kunnen niet worden uitgevoerd of geopend; daardoor is er geen infectiegevaar meer. Zie "*Bestanden in quarantaine beheren*" (p. 93) voor meer informatie.

  Belangrijk

  Voor specifieke types bedreigingen is desinfectie niet mogelijk omdat het gedetecteerde bestand volledig boosaardig is. In dergelijke gevallen wordt het geïnfecteerde bestand verwijderd van de schijf.

- **Verdachte bestanden.** Soms worden bestanden door de heuristische analyse aangemerkt als 'verdacht'. Verdachte bestanden kunnen niet worden gedesinfecteerd, omdat hiervoor geen standaard desinfectieroutine bestaat. Ze worden verplaatst naar quarantaine om een mogelijke infectie te voorkomen.

  Bestanden in quarantaine worden standaard automatisch verzonden naar Bitdefender Labs voor analyse door de bedreigingsonderzoekers van Bitdefender. Wanneer de aanwezigheid van een bedreiging wordt bevestigd, wordt een informatie-update voor bedreigingen uitgegeven zodat de bedreiging kan worden verwijderd.

- **Archieven die geïnfecteerde bestanden bevatten.**
  - Archieven die alleen geïnfecteerde bestanden bevatten, worden automatisch verwijderd.
  - Als een archief zowel geïnfecteerde als schone bestanden bevat, zal Bitdefender proberen de geïnfecteerde bestanden te verwijderen op voorwaarde dat het programma het archief met de schone bestanden opnieuw kan opbouwen. Als het niet mogelijk is het

archief te reconstrueren, wordt u op de hoogte gebracht dat er geen actie kan worden ondernomen om zo te vermijden dat schone bestanden verloren gaan.

Naar quarantaine
Verplaatst gedetecteerde bestanden naar de quarantaine. In quarantaine geplaatst bestanden kunnen niet worden uitgevoerd of geopend; daardoor is er geen infectiegevaar meer. Zie "*Bestanden in quarantaine beheren*" (p. 93) voor meer informatie.

Toegang weigeren
Wanneer een geïnfecteerd bestand is gedetecteerd, zal de toegang tot dit bestand worden geweigerd.

13.1.3. De standaardinstellingen herstellen

De standaardinstellingen voor de realtime-beveiliging garanderen een goede beveiliging tegen bedreigingen, met een minimale impact op de systeemprestaties.

De standaard real time-beveiligingsinstellingen herstellen:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Bescherming**.
2. In het deelvenster **ANTIVIRUS** klikt u op **Openen**.
3. In het venster **Geavanceerd** scrolt u naar beneden tot u de optie **Geavanceerde instellingen resetten** ziet. Selecteer deze optie om de antivirusinstellingen terug te stellen naar fabrieksinstellingen.

13.2. Scannen op aanvraag

Bitdefender heeft als hoofddoel uw apparaat vrij te houden van bedreigingen. Dit wordt gedaan door nieuwe bedreigingen uit uw apparaat weg te houden en door uw e-mailberichten en alle nieuwe bestanden, die u downloadt of kopieert naar uw systeem, te scannen.

Het risico bestaat dat een bedreiging zich reeds in uw systeem heeft genesteld voordat u Bitdefender installeert. Het is dan ook een bijzonder goed idee uw apparaat meteen te scannen op aanwezige bedreigingen nadat u Bitdefender hebt geïnstalleerd. En het is absoluut een goed idee om uw apparaat regelmatig te scannen op bedreigingen.

Scannen op aanvraag is gebaseerd op scantaken. Scantaken bepalen de scanopties en de objecten die moeten worden gescand. U kunt de apparaat

scannen wanneer u dat wilt door de standaardtaken of uw eigen scantaken (door gebruiker gedefinieerde taken) uit te voeren. Als u specifieke locaties wilt scannen op uw apparaat of de scanopties wilt configureren, kunt u een aangepaste scantaak configureren en uitvoeren.

13.2.1. Een bestand of map scannen op bedreigingen

U moet bestanden en mappen scannen wanneer u vermoedt dat ze geïnfecteerd zijn. Klik met de rechtermuisknop op het bestand of de map die u wilt scannen, kies **Bitdefender** en selecteer **Scannen met Bitdefender**. De Antivirusscanwizard wordt weergegeven en begeleidt u doorheen het scanproces. Aan het einde van de scan wordt u gevraagd te kiezen welke acties moeten worden ondernemen op de gedetecteerde bestanden, als die er zijn.

13.2.2. Een snelle scan uitvoeren

Quick Scan gebruikt in-the-cloud scanning om bedreigingen die op uw systeem worden uitgevoerd, te detecteren. Het uitvoeren van een Snelle scan duurt doorgaans minder dan een minuut en gebruikt slechts een fractie van het systeemgeheugen dat gewone antivirusscans gebruiken.

Een snelle scan starten:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Bescherming**.
2. In het deelvenster **ANTIVIRUS** klikt u op **Openen**.
3. In de vensters **Scans** klikt u op de knop **Scan uitvoeren** naast **Snelle scan**.
4. Volg de Antivirusscanwizard om de scan te voltooien. Bitdefender zal automatisch de aanbevolen acties ondernemen op de gedetecteerde bestanden. Als er niet opgeloste bedreigingen achterblijven, wordt u gevraagd de acties te kiezen die moeten worden ondernomen.

13.2.3. Een systeemscan uitvoeren

De systeemscan scant de volledige apparaaten op alle types bedreigingen die de beveiliging in gevaar brengen, zoals malware, spyware, adware, rootkits en andere.

Opmerking
Omdat **Systeemscan** een grondige scan van het complete systeem uitvoert, kan de scan even duren. Het is daarom aanbevolen deze taak uit te voeren wanneer u de apparaaten niet gebruikt.

Voordat u een systeemscan uitvoert, wordt het volgende aanbevolen:

- Zorg ervoor dat Bitdefender up to date is met de informatiedatabase voor bedreigingen. Het scannen van uw apparaat met een oude informatiedatabase voor bedreigingen kan verhinderen dat Bitdefender nieuwe bedreigingen die sinds de laatste update zijn gevonden, detecteert. Zie "*Bitdefender up-to-date houden*" (p. 40) voor meer informatie.
- Alle open programma's afsluiten

Als u specifieke locaties wilt scannen op uw apparaat of de scanopties wilt configureren, kunt u een aangepaste scantaak configureren en uitvoeren. Zie "*Een aangepaste scan configureren*" (p. 81) voor meer informatie.

Een systeemscan lanceren:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Bescherming**.
2. In het deelvenster **ANTIVIRUS** klikt u op **Openen**.
3. In de vensters **Scans** klikt u op de knop **Scan uitvoeren** naast **Systeemscan**.
4. De eerste keer dat u de Systeemscan uitvoert, krijgt u een inleiding. Klik op **OK, BEGREPEN** om verder te gaan.
5. Volg de Antivirusscanwizard om de scan te voltooien. Bitdefender zal automatisch de aanbevolen acties ondernemen op de gedetecteerde bestanden. Als er niet opgeloste bedreigingen achterblijven, wordt u gevraagd de acties te kiezen die moeten worden ondernomen.

13.2.4. Een aangepaste scan configureren

In het venster **Scans beheren** kunt u Bitdefender zo instellen dat het scans uitvoert wanneer u denkt dat uw apparaat op mogelijke bedreigingen moet worden gecontroleerd. U kunt ervoor kiezen om een Systeemscan of Snelle scan in te plannen, of u kunt een aangepaste scan aanmaken.

Om een nieuwe aangepaste scan in detail te configureren:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Bescherming**.
2. In het deelvenster **ANTIVIRUS** klikt u op **Openen**.

3. In de vensters **Scans** klikt u op **+Scan maken**.
4. Voer in het veld **Taaknaam** een naam in voor de scan, selecteer vervolgens de locaties die u wilt laten scannen en klik op **Volgende**.
5. Configureer deze algemene opties:
   - **Enkel toepassingen scannen**. U kunt Bitdefender zo instellen dat enkel toepassingen waartoe toegang wordt gezocht, worden gescand.
   - **Prioriteit scantaak**. U kunt kiezen welke impact een scanprocedure mag hebben op de prestaties van uw systeem.
     - Auto - De prioriteit van de scanprocedure hangt af van de systeemactiviteit. Om te verzekeren dat de scanprocedure geen invloed heeft op de systeemactiviteit, beslist Bitdefender of de scanprocedure met een hoge of lage prioriteit moet worden uitgevoerd.
     - Hoog - De prioriteit van de scanprocedure is hoog. Door deze optie te selecteren, laat u andere programma's trager werken, en verkort u de tijd die nodig is om de scanprocedure te voltooien.
     - Laag - De prioriteit van de scanprocedure is laag. Door deze optie te selecteren, laat u andere programma's sneller werken, en verlengt u de tijd die nodig is om de scanprocedure te voltooien.
   - **Acties na het scannen**. Kies welke actie Bitdefender moet ondernemen als er geen bedreigingen zijn gevonden:
     - Venster met samenvatting weergeven
     - Apparaat uitschakelen
     - Scanvenster sluiten
6. Als u de scanopties in detail wilt configureren, klikt u op **Geavanceerde opties weergeven**. U vindt informatie over de vermelde scans aan het einde van dit gedeelte.

   Klik op **Volgende**.
7. U kunt **Scantaak inplannen** indien gewenst inschakelen, en dan kiezen wanneer de aangepaste scan die u hebt gemaakt, moet beginnen.
   - Bij opstarten systeem
   - Dagelijks

- Maandelijks
- Wekelijks

Kiest u Dagelijks, Maandelijks of Wekelijks, versleept u de schuifregelaar op de schaal om te kiezen wanneer de ingeplande scan moet starten.

8. Klik op **OPSLAAN** om de instellingen op te slaan en sluit het configuratievenster.

   Afhankelijk van de locaties die moeten worden gescand, kan het scannen even duren. Indien er tijdens de scanprocedure bedreigingen worden gevonden, wordt u gevraagd de acties te kiezen die in verband met de gedetecteerde bestanden moeten worden ondernomen.

Informatie over de scanopties

Deze informatie kan nuttig zijn:

- Als u bepaalde termen niet kent, kunt u ze opzoeken in de woordenlijst. U kunt ook nuttige informatie vinden door op het Internet te zoeken.
- **Mogelijk ongewenste toepassingen scannen.** Selecteer deze optie om te scannen op ongewenste toepassingen. Een PUA (potentially unwanted application) of PUP (potentially unwanted program) is software die meestal wordt samengebundeld met freeware software en pop-ups weergeeft of een werkbalk in de standaardbrowser installeert. Sommige PUA's of PUP's veranderen de homepage of zoekmotor, anderen voeren op de achtergrond meerdere processen uit waardoor uw pc vertraagt of laten talrijke advertenties zien. Deze programma's kunnen zonder uw toestemming worden geïnstalleerd (ook wel adware genoemd) of worden standaard toegevoegd aan de uitdrukkelijke installatiekit (advertentie-ondersteund).
- **Archieven scannen.** Archieven die geïnfecteerde bestanden bevatten, zijn geen onmiddellijke bedreiging voor de beveiliging van uw systeem. De bedreiging kan uw systeem alleen beïnvloeden als het geïnfecteerde bestand wordt uitgepakt uit het archief en uitgevoerd zonder dat de real time-beveiliging is ingeschakeld. Het is echter aanbevolen deze optie te gebruiken om eventuele potentiële bedreigingen te detecteren en te verwijderen, zelfs als het niet om een onmiddellijke bedreiging gaat.

  Versleep de schuifregelaar langs de schaal om archieven die groter zijn dan een bepaalde waarde in MB (Megabytes) uit te sluiten.

Opmerking
Als gearchiveerde bestanden worden gescand, duurt het scannen langer en worden er meer systeembronnen gebruikt.

- **Enkel nieuwe en gewijzigde bestanden scannen.** Door alleen nieuwe en gewijzigde bestanden te scannen, kunt u de algemene reactiviteit van uw systeem aanzienlijk verbeteren met een minimale inlevering op het vlak van beveiliging.
- **Opstartsectoren scannen.** U kunt Bitdefender instellen om de startgebieden van uw harde schijf te scannen. Dit deel van de harde schijf bevat de vereiste computercode om het opstartproces te starten. Als een bedreiging het opstartgebied besmet, kan de toegang tot de schijf geblokkeerd worden en het is mogelijk dat u dan uw systeem niet meer kunt starten en geen toegang meer hebt tot uw gegevens.
- **Geheugen scannen.** Selecteer deze optie om programma's te scannen die worden uitgevoerd in uw systeemgeheugen.
- **Register scannen.** Selecteer deze optie voor het scannen van registersleutels. Het Windows-register is een database die de configuratie-instellingen en opties opslaat voor de componenten van het Windows-besturingssysteem, evenals voor geïnstalleerde toepassingen.
- **Cookies scannen.** Selecteer deze opties om de cookies te scannen die via browsers op uw apparaaten zijn opgeslagen.
- **Keyloggers scannen.** Selecteer deze optie om uw systeem te scannen op keyloggers. Keyloggers slaan op wat u op uw toetsenbord intypt en zenden via Internet verslagen naar een kwaadwillend persoon (hacker). De hacker kan gevoelige informatie uit de gestolen data halen, zoals bankrekeningnummers en wachtwoorden, en deze voor zijn eigen doeleinden gebruiken.

13.2.5. Antivirusscanwizard

Telkens wanneer u een scan op aanvraag start (bijvoorbeeld klik met de rechtermuisknop op een map, kies Bitdefender en selecteer **Scannen met Bitdefender**), verschijnt de Antivirusscanwizard van Bitdefender. Volg de wizard om het scannen te voltooien.

Opmerking

Als de scanwizard niet verschijnt, kan de scan worden geconfigureerd om stil te worden uitgevoerd op de achtergrond. Zoek het pictogram voor de scanvoortgang in het systeemvak. U kunt op dit pictogram klikken om het scanvenster te openen en de scanvoortgang te bekijken.

Stap 1 - Scan uitvoeren

Bitdefender start het scannen van de geselecteerde objecten. U ziet real time-informatie over de scanstatus en statistieken (inclusief de verstreken tijd, een schatting van de resterende tijd en het aantal gedetecteerde bedreigingen).

Wacht tot Bitdefender klaar is met scannen. Afhankelijk van de complexiteit van de scan, kan het scanproces enige tijd in beslag nemen.

De scan stoppen of pauzeren. U kunt het scannen op elk ogenblik stoppen door op **STOP** te klikken. U gaat dan rechtstreeks naar de laatste stap van de wizard. Klik op **PAUZE** om het scanproces tijdelijk te stoppen. Om het scannen te hervatten, klikt u op **HERVATTEN**.

Wachtwoordbeveiligde archieven. Wanneer een met een wachtwoord beschermd archief wordt gedetecteerd, kunt u afhankelijk van de scaninstellingen worden gevraagd het wachtwoord op te geven. Met een wachtwoord beveiligde archieven kunnen niet worden gescand, tenzij u het wachtwoord opgeeft. De volgende opties zijn beschikbaar:

- **Wachtwoord.** Als u wilt dat Bitdefender het archief scant, moet u deze optie selecteren en het wachtwoord invoeren. Als u het wachtwoord niet kent, kies dan een van de andere opties.
- **Geen wachtwoord vragen en dit object overslaan bij het scannen.** Selecteer deze optie om het scannen van dit archief over te slaan.
- **Alle wachtwoordbeveiligde items overslaan zonder ze te scannen.** Selecteer deze optie als u niet wilt worden lastig gevallen met betrekking tot wachtwoordbeveiligde archieven. Bitdefender zal ze niet kunnen scannen, maar er wordt wel een gegeven bewaard in het scanlogboek.

Kies de gewenste optie en klik op **OK** om door te gaan met scannen.

Stap 2 – Acties kiezen

Aan het einde van de scan wordt u gevraagd te kiezen welke acties moeten worden ondernemen op de gedetecteerde bestanden, als die er zijn.

Opmerking

Wanneer u een snelle scan of een systeemscan uitvoert, neemt Bitdefender automatisch de aanbevolen acties op bestanden die zijn gedetecteerd tijdens de scan. Als er niet opgeloste bedreigingen achterblijven, wordt u gevraagd de acties te kiezen die moeten worden ondernomen.

De geïnfecteerde objecten worden weergegeven in groepen, die zijn gebaseerd op de bedreigingen waarmee ze zijn geïnfecteerd. Klik op de link van de bedreiging voor meer informatie over de geïnfecteerde objecten.

U kan een algemene actie selecteren die moet worden genomen voor alle groepen problemen of u kan afzonderlijke acties voor elke groep problemen selecteren. Een of meerdere van de volgende opties kunnen in het menu verschijnen.

Neem gepaste acties

Bitdefender zal de aanbevolen acties ondernemen op basis van het type van het gedetecteerde bestand:

- **Geïnfecteerde bestanden.** Bestanden die als besmet zijn gedetecteerd, komen overeen met een stukje bedreigingsinformatie gevonden in de informatiedatabase voor bedreigingen van Bitdefender. Bitdefender zal automatisch proberen de kwaadaardige code van een geïnfecteerd bestand te verwijderen en het originele bestand te reconstrueren. Deze bewerking wordt 'desinfecteren' genoemd.

  Bestanden die niet kunnen worden gedesinfecteerd, worden naar quarantaine verplaatst om de infectie in te dammen. In quarantaine geplaatst bestanden kunnen niet worden uitgevoerd of geopend; daardoor is er geen infectiegevaar meer. Zie "*Bestanden in quarantaine beheren*" (p. 93) voor meer informatie.

  ### Belangrijk

  Voor specifieke types bedreigingen is desinfectie niet mogelijk omdat het gedetecteerde bestand volledig boosaardig is. In dergelijke gevallen wordt het geïnfecteerde bestand verwijderd van de schijf.

- **Verdachte bestanden.** Soms worden bestanden door de heuristische analyse aangemerkt als 'verdacht'. Verdachte bestanden kunnen niet worden gedesinfecteerd, omdat hiervoor geen standaard desinfectieroutine bestaat. Ze worden verplaatst naar quarantaine om een mogelijke infectie te voorkomen.

Bestanden in quarantaine worden standaard automatisch verzonden naar Bitdefender Labs voor analyse door de bedreigingsonderzoekers van Bitdefender. Wanneer de aanwezigheid van een bedreiging wordt bevestigd, wordt een informatie-update uitgegeven zodat de bedreiging kan worden verwijderd.

- **Archieven die geïnfecteerde bestanden bevatten.**
  - Archieven die alleen geïnfecteerde bestanden bevatten, worden automatisch verwijderd.
  - Als een archief zowel geïnfecteerde als schone bestanden bevat, zal Bitdefender proberen de geïnfecteerde bestanden te verwijderen op voorwaarde dat het programma het archief met de schone bestanden opnieuw kan opbouwen. Als het niet mogelijk is het archief te reconstrueren, wordt u op de hoogte gebracht dat er geen actie kan worden ondernomen om zo te vermijden dat schone bestanden verloren gaan.

Wissen

Verwijdert gedetecteerde bestanden van de schijf.

Als er geïnfecteerde bestanden samen met schone bestanden in een archief zijn opgeslagen, zal Bitdefender proberen de geïnfecteerde bestanden te verwijderen en het archief opnieuw op te bouwen met de schone bestanden. Als het niet mogelijk is het archief te reconstrueren, wordt u op de hoogte gebracht dat er geen actie kan worden ondernomen om zo te vermijden dat schone bestanden verloren gaan.

Geen actie nemen

Er wordt geen actie ondernomen voor de geïnfecteerde bestanden. Als de scan is voltooid, kan u het scanlogbestand openen om informatie over deze bestanden te zien.

Klik op **Doorgaan** om de aangegeven acties toe te passen.

Stap 3 – Overzicht

Wanneer Bitdefender het oplossen van de problemen heeft voltooid, verschijnen de scanresultaten in een nieuw venster. Als u uitgebreide informatie over het scanproces wenst, klikt u op **LOGBOEK WEERGEVEN** om het scanlogboek weer te geven.

Belangrijk

In de meeste gevallen desinfecteert Bitdefender met succes de geïnfecteerde bestanden die het detecteert of isoleert het de infectie. Er zijn echter problemen die niet automatisch kunnen worden opgelost. Start indien nodig uw systeem opnieuw, zodat het installatieprogramma de installatie kan voltooien. Meer informatie en instructies over het handmatig verwijderen van een bedreiging vindt u onder "*Bedreigingen van uw systeem verwijderen*" (p. 157).

13.2.6. Scanlogboeken controleren

Telkens wanneer er een scan wordt uitgevoerd, wordt er een scanverslag aangemaakt en Bitdefender slaat de gedetecteerde problemen op in het Antivirusvenster. Het scanlog bevat gedetailleerde informatie over het gevolgde scanproces, zoals de scanopties, het scandoel, de gevonden bedreigingen en de hierop uitgevoerde acties.

Zodra het scannen is voltooid, kunt u het scanlogboek direct vanaf de scanwizard openen door op **LOGBOEK WEERGEVEN** te klikken.

Een scanlog of een gedetecteerde infectie later bekijken:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Notificaties**.
2. In het tabblad **Alle** selecteert u de kennisgeving betreffende de recentste scan.

   Hier vindt u alle gebeurtenissen van scans op bedreigingen, inclusief bedreigingen die zijn gedetecteerd door Scannen bij toegang, door gebruiker gestarte scans en statuswijzigingen voor automatische scans.
3. In de kennisgevingenlijst kunt u controleren welke scans onlangs werden uitgevoerd. Klik op een kennisgeving om details erover weer te geven.
4. Klik op **Logboek weergeven** om het scanlogboek te openen.

13.3. Automatisch scannen van verwisselbare media

Bitdefender detecteert automatisch wanneer u een verwisselbaar opslagapparaat aansluit op uw apparaat en scant dit op de achtergrond wanneer de Autoscan-optie geactiveerd is. Dit is aanbevolen om infecties van uw apparaat door bedreigingen te voorkomen.

Gedetecteerde apparaten vallen in een van deze categorieën:

- Cd's/dvd's
- USB-sticks zoals flashpennen en externe harde schijven

- toegewezen (externe) netwerkstations

U kunt het automatisch scannen afzonderlijk configureren voor elke categorie opslagapparaten. Automatisch scannen van toegewezen netwerkstations is standaard uitgeschakeld.

13.3.1. Hoe werkt het?

Wanneer Bitdefender een verwisselbaar opslagapparaat detecteert, begint het het apparaat te scannen op bedreigingen (op voorwaarde dat de automatische scan voor dat type apparaat is ingeschakeld). U wordt via een pop-upvenster gemeld dat een nieuw apparaat is gedetecteerd en dat het wordt gescand.

Een Bitdefender-scanpictogram verschijnt in het systeemvak. U kunt op dit pictogram klikken om het scanvenster te openen en de scanvoortgang te bekijken.

Nadat de scan is voltooid, wordt het venster met de scanresultaten weergegeven om u te laten weten of u de bestanden op de verwisselbare media veilig kunt openen.

In de meeste gevallen verwijdert Bitdefender automatisch de gedetecteerde bedreigingen of isoleert het programma geïnfecteerde bestanden in quarantaine. Als er na de scan niet opgeloste bedreigingen zijn, wordt u gevraagd de acties te kiezen die moeten worden ondernomen.

Opmerking

Houd ermee rekening dat er geen actie kan worden ondernomen op geïnfecteerde of verdachte bestanden die op cd's/dvd's zijn gevonden. Zo kan er ook geen actie worden ondernemen op geïnfecteerde of verdachte bestanden die zijn gedetecteerd op toegewezen netwerkstations als u niet over de geschikte privileges beschikt.

Deze informatie kan nuttig zijn voor u:

- Wees voorzichtig wanneer u een cd/dvd gebruikt die besmet is met een bedreiging. De bedreiging kan niet van de schijf worden verwijderd (het medium is alleen-lezen). Zorg dat de real time-beveiliging is ingeschakeld om te verhinderen dat bedreigingen zich over uw systeem verspreiden. De beste werkwijze is het kopiëren van alle waardevolle gegevens van de schijf naar uw systeem en ze daarna verwijderen van de schijf.

- In sommige gevallen zal Bitdefender niet in staat zijn bedreigingen te verwijderen uit specifieke bestanden vanwege wettelijke of technische beperkingen. Een voorbeeld hiervan zijn bestanden die gearchiveerd zijn met een eigen technologie (dit is te wijten aan het feit dat het archief niet correct opnieuw kan worden gemaakt).

  Om te weten hoe u met bedreigingen moet omgaan, ga naar "*Bedreigingen van uw systeem verwijderen*" (p. 157).

13.3.2. Scan verwisselbare media beheren

Automatische scans van verwisselbare media beheren:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Bescherming**.
2. In het deelvenster **ANTIVIRUS** klikt u op **Openen**.
3. Selecteer het venster **Instellingen**.

De scanopties zijn vooraf geconfigureerd voor de beste detectieresultaten. Als er geïnfecteerde bestanden wordt gedetecteerd, probeert Bitdefender ze te desinfecteren (de kwaadaardige code verwijderen) of ze naar quarantaine te verplaatsen. Als beide acties mislukken, kunt u met de Antivirusscanwizard andere acties opgeven die moeten worden ondernemen op geïnfecteerde bestanden. De scanopties zijn standaard en u kunt ze niet wijzigen.

Voor de beste beveiliging is het aanbevolen om de geselecteerde optie van **Autoscan** in te schakelen voor alle types verwisselbare opslagapparaten.

13.4. Gastbestand scannen

Het gastbestand zit standaard in de installatie van uw besturingssysteem en wordt gebruik om hostnamen aan IP-adressen te koppelen, telkens wanneer u een nieuwe webpagina bezoekt, een verbinding maakt met een FTP of andere internetservers. Het is een gewoon tekstbestand en kwaadaardige programma's zouden het kunnen wijzigen. Geavanceerde gebruikers weten hoe ze het moeten gebruiken om vervelende advertenties, banners, cookies van derden of overvallers te blokkeren.

Om scan-gastbestanden te configureren:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Instellingen**.
2. Klik op het tabblad **Geavanceerd**.
3. Schakel **Gastbestand scannen** in of uit.

13.5. Scanuitsluitingen configureren

Met Bitdefender kunt u specifieke bestanden, mappen of bestandsextensies uitsluiten van het scannen. Deze functie is bedoeld om te vermijden dat u in uw werk wordt gestoord en kan ook helpen de systeemprestaties te verbeteren. Uitsluitingen zijn voorzien voor gebruikers die over een gevorderde computerkennis beschikken. Als u deze kennis niet hebt, kunt u de aanbevelingen van een Bitdefender-vertegenwoordiger volgen.

U kunt de uitsluitingen configureren die u wilt toepassen op Scannen bij toegang of Scannen op aanvraag afzonderlijk, of op beide scantypes tegelijk. De objecten die zijn uitgesloten van scannen bij toegang, worden niet gescand, ongeacht of ze door u of door een toepassing worden geopend.

Opmerking

Uitzonderingen komen NIET in aanmerking voor contextueel scannen. Contextueel scannen is een type van scannen op aanvraag. Klik met de rechtermuisknop op het bestand of de map die u wilt scannen en selecteer **Scannen met Bitdefender**.

13.5.1. Bestanden en mappen uitsluiten van het scannen

Om specifieke bestanden en mappen van het scannen uit te sluiten:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Bescherming**.
2. In het deelvenster **ANTIVIRUS** klikt u op **Openen**.
3. Klik in het venster **Instellingen** op **Uitzonderingen beheren**.
4. Klik op **+Een uitzondering toevoegen**.
5. Voer in het overeenkomende veld het pad in van de map die u wilt uitsluiten van het scannen.

   U kunt ook naar de map navigeren door te klikken op de knop Bladeren aan de rechterkant van de interface. Selecteer de map en klik op **OK**.
6. Schakel de schakelaar naast de beschermingsvoorziening die de map niet moet scannen, in. Er zijn drie opties:
   - Antivirus
   - Preventie van online dreigingen
   - Advanced Threat Defense

7. Klik op **Opslaan** om de wijzigingen op te slaan en het venster te sluiten.

13.5.2. Bestandsextensies uitsluiten van scannen

Wanneer u een bestandsextensie uitsluit van de scan, zal Bitdefender bestanden met die extensie niet meer scannen, ongeacht hun locatie op uw apparaat. De uitsluiting is ook van toepassing op bestanden op verwisselbare media, zoals cd's, dvd's, USB-opslagapparaten of netwerkstations.

> **Belangrijk**
> Ga voorzichtig te werk wanneer u extensies uitsluit van het scannen, want dergelijke uitsluitingen kunnen uw apparaat kwetsbaar maken voor bedreigingen.

Om bestandsextensies uit te sluiten van het scannen:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Bescherming**.
2. In het deelvenster **ANTIVIRUS** klikt u op **Openen**.
3. Klik in het venster **Instellingen** op **Uitzonderingen beheren**.
4. Klik op **+Een uitzondering toevoegen**.
5. Voer de extensies in die u van het scannen wilt uitsluiten met een puntje ervoor, en scheid ze van elkaar met puntkomma's (;).

   txt;avi;jpg
6. Schakel de schakelaar naast de beschermingsvoorziening die de extensie niet moet scannen, in.
7. Klik op **Opslaan**.

13.5.3. Scanuitsluitingen beheren

Als de geconfigureerde scanuitsluitingen niet langer nodig zijn, is het aanbevolen dat u ze verwijdert of dat u scanuitsluitingen uitschakelt.

Om scanuitsluitingen te beheren:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Bescherming**.
2. In het deelvenster **ANTIVIRUS** klikt u op **Openen**.
3. Klik in het venster **Instellingen** op **Uitzonderingen beheren**. Er wordt een lijst met al uw uitzonderingen weergegeven.

4. Klik op een van de beschikbare knoppen om scanuitzonderingen te verwijderen of te bewerken. Ga als volgt te werk:

   - Om iets uit de lijst te verwijderen, klik op de knop ernaast.
   - Om een gegeven in de tabel te bewerken, klikt u ernaast op de knop **Bewerken**. Er verschijnt een nieuw venster. Hierin kunt u de extensie of het pad dat moet worden uitgezonderd, wijzigen, alsook de beveiligingsvoorziening die de extensie of het pad moet uitsluiten. Breng de nodige wijzigingen aan en klik daarna op **WIJZIGEN**.

13.6. Bestanden in quarantaine beheren

Bitdefender isoleert de door bedreigingen geïnfecteerde bestanden die het niet kan desinfecteren en de verdachte bestanden in een beveiligd gebied dat de quarantaine wordt genoemd. Wanneer een bedreiging in quarantaine is, kan het geen schade berokkenen, aangezien het niet kan worden uitgevoerd of gelezen.

Bestanden in quarantaine worden standaard automatisch verzonden naar Bitdefender Labs voor analyse door de bedreigingsonderzoekers van Bitdefender. Wanneer de aanwezigheid van een bedreiging wordt bevestigd, wordt een informatie-update uitgegeven zodat de bedreiging kan worden verwijderd.

Daarnaast scant Bitdefender de bestanden in quarantaine telkens de informatiedatabase voor bedreigingen geüpdatet wordt. Opgeruimde bestanden worden automatisch terug naar hun originele locatie verplaatst.

De bestanden in quarantaine controleren en beheren:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Bescherming**.
2. In het deelvenster **ANTIVIRUS** klikt u op **Openen**.
3. Ga naar het venster **Instellingen**.

   Hier ziet u de naam van de bestanden in quarantaine, alsook hun oorspronkelijke locatie en de naam van de gedetecteerde bedreigingen.
4. Bestanden in quarantaine worden automatisch beheerd door Bitdefender op basis van de standaard quarantaine-instellingen.

   Hoewel dit niet wordt aanbevolen, kunt u de quarantaine-instellingen aanpassen volgens uw voorkeur door te klikken op **Instellingen weergeven**.

   Klik op de schakelaars om deze optie in of uit te schakelen.

Quarantaine opnieuw scannen na update dreigingsinformatie
Houd deze optie ingeschakeld om bestanden in quarantaine automatisch te scannen na elke update van de informatiedatabase voor bedreigingen. Opgeruimde bestanden worden automatisch terug naar hun originele locatie verplaatst.

Inhoud ouder dan 30 dagen verwijderen
Bestanden in quarantaine die ouder zijn dan 30 dagen worden automatisch verwijderd.

Maak uitzonderingen aan voor herstelde bestanden
De bestanden die u vanuit quarantaine herstelt, worden zonder reparatie teruggezet naar hun oorspronkelijke locatie, en worden voor volgende scans automatisch uitgesloten.

5. Om een bestand in quarantaine te verwijderen, selecteert u het en klikt u op de knop **Verwijderen**. Als u een bestand uit de quarantaine wilt terugzetten naar de oorspronkelijke locatie, selecteert u het bestand en klikt u op **Terugzetten**.

14. ADVANCED THREAT DEFENSE

Bitdefender Geavanceerde dreigingscontrole is een innovatieve proactieve detectietechnologie die geavanceerde heuristische methoden gebruikt voor het in real time detecteren van ransomware en andere nieuwe potentiële bedreigingen.

Geavanceerde dreigingscontrole bewaakt voortdurend de toepassingen die op de apparaat worden uitgevoerd en zoekt naar acties die op bedreigingen lijken. Elk van deze acties krijgt een score en voor elk proces wordt een algemene score berekend.

Als veiligheidsmaatregel wordt u op de hoogte gesteld telkens er bedreigingen of mogelijk kwaadwillige processen worden gedetecteerd en geblokkeerd.

14.1. Advanced Threat Defense in- of uitschakelen

Advanced Threat Defense in- of uitschakelen:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Bescherming**.
2. Klik op **Instellingen** in het venster **ADVANCED THREAT DEFENSE**.
3. Ga naar het venster **Instellingen** en klik op de schakelaar naast **Bitdefender Advanced Threat Defense**.

Opmerking

Om uw systeem beschermd te houden tegen ransomware en andere bedreigingen, bevelen we u aan Advanced Threat Defense zo weinig mogelijk uit te schakelen.

14.2. Gedetecteerde kwaadwillige aanvallen controleren

Wanneer bedreigingen of mogelijk kwaadwillige processen worden gedetecteerd, blokkeert Bitdefender deze om uw apparaat te beschermen tegen ransomware of andere malware. U kunt de lijst met gedetecteerde kwaadwillige aanvallen op elk gewenst moment controleren aan de hand van de onderstaande stappen:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Bescherming**.
2. Klik op **Instellingen** in het venster **ADVANCED THREAT DEFENSE**.

3. Ga naar het venster **Threat Defense**.

   De aanvallen die de voorbije 90 dagen werden gedetecteerd, worden getoond. Om meer informatie te lezen over de opgespoorde ransomware, de paden van het schadelijke proces en of het onschadelijk maken met succes werd uitgevoerd, kunt u er gewoon op klikken.

14.3. Processen toevoegen aan uitzonderingen

U kunt uitzonderingsregels configureren voor vertrouwde toepassingen zodat Advanced Threat Defense ze niet blokkeert als ze acties uitvoeren die op bedreigingen lijken.

Om processen toe te voegen aan de uitsluitingenlijst van Advanced Threat Defense:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Bescherming**.
2. Klik op **Instellingen** in het venster **ADVANCED THREAT DEFENSE**.
3. Klik in het venster **Instellingen** op **Uitzonderingen beheren**.
4. Klik op **+Een uitzondering toevoegen**.
5. Voer in het overeenkomende veld het pad in van de map die u wilt uitsluiten van het scannen.

   U kunt ook naar het uitvoerbare bestand navigeren door te klikken op de knop Bladeren aan de rechterkant van de interface. Selecteer het bestand en klik op **OK**.
6. Schakel de schakelaar naast **Advanced Threat Defense** in.
7. Klik op **Opslaan**.

14.4. Detectie van exploits

Een manier voor hackers om in te breken in systemen, is misbruik maken van specifieke bugs of kwetsbaarheden in computersoftware (toepassingen of plug-ins) en hardware. Om te garanderen dat uw apparaat vrij blijft van dergelijke aanvallen, die zich meestal heel snel verspreiden, maakt Bitdefender gebruik van de meest recente anti-exploittechnologieën.

Detectie van exploit in- en uitschakelen

Om detectie van exploits in en uit te schakelen:

- Klik in het navigatiemenu in de Bitdefender-interface op **Bescherming**.
- Klik op **Instellingen** in het venster **ADVANCED THREAT DEFENSE**.
- Ga naar het venster **Instellingen** en klik op de schakelaar naast **Detectie exploits** om de voorziening in of uit te schakelen.

Opmerking
De optie Detectie van exploits is standaard ingeschakeld.

15. PREVENTIE VAN ONLINE DREIGINGEN

Bitdefender Online Threat Prevention garandeert een veilige surfervaring door u te waarschuwen over mogelijke kwaadaardige websites.

Bitdefender biedt realtime bescherming tegen online bedreigingen voor:

- Internet Explorer
- Microsoft Edge
- Mozilla Firefox
- Google Chrome
- Safari
- Bitdefender Safepay™
- Opera

Om de instellingen van Online Threat Prevention te configureren:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Bescherming**.
2. Klik in het venster **ONLINE THREAT PREVENTION** op **Instellingen**.

In de secties **Webbescherming** klikt u op de aan-uitschakelaars voor:

- Web attack prevention blokkeert bedreigingen die via het internet binnenkomen, met inbegrip van drive-by downloads.
- Search advisor is een component die de resultaten van uw zoekopdrachten en de koppelingen die op websites van sociale netwerken zijn geplaatst, beoordeelt door naast elk resultaat een pictogram te plaatsen.

  U mag deze webpagina niet bezoeken.

  Deze webpagina bevat mogelijke gevaarlijke onderdelen. Wees voorzichtig als deze pagina toch wilt bezoeken.

  Dit is een pagina die u veilig kunt bezoeken.

  Search Advisor beoordeelt de zoekresultaten van de volgende zoekmachines op Internet:
  - Google
  - Yahoo!
  - Bing
  - Baidu

  Search Advisor beoordeelt de koppelingen die zijn geplaatst op de volgende online sociale netwerkservices:

- Facebook
- Twitter

- Versleutelde webscan.

  Meer verfijnde aanvallen kunnen gebruik maken van beveiligd webverkeer om hun slachtoffers te misleiden. We raden u dan ook aan om de optie Versleutelde Webscan ingeschakeld te laten.

- Bescherming tegen fraude.
- Bescherming tegen phishing.

Scrol naar beneden tot u bij de sectie **Network Threat Prevention** komt. Hier vindt u de optie **Network Threat Prevention**. Houd deze optie ingeschakeld om uw apparaat te beschermen tegen aanvallen van complexe malware (zoals ransomware) op basis van kwetsbaarheden.

U kunt een lijst opmaken van websites, domeinen en IP-adressen die niet zullen worden gescand door de antibedreiging-, antiphishing- en antifraude-engines van Bitdefender. De lijst dient enkel de websites, domeinen en IP-adressen te bevatten die u volledig vertrouwt.

Om websites, domeinen en IP-adressen via de functie Online Threat Prevention van Bitdefender te configureren en te beheren:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Bescherming**.
2. Klik in het venster **ONLINE THREAT PREVENTION** op **Instellingen**.
3. Klik op **Uitzonderingen beheren**.
4. Klik op **+Een uitzondering toevoegen**.
5. Voer in het overeenkomende veld de naam van de website of van het domein of het IP-adres in dat u wilt toevoegen aan de uitzonderingen.
6. Klik op de schakelaar naast **Online Threat Prevention**.
7. Om iets uit de lijst te verwijderen, klik op de knop ernaast.

   Klik op **Opslaan** om de wijzigingen op te slaan en het venster te sluiten.

15.1. Bitdefender waarschuwt in de browser

Telkens wanneer u een website bezoekt die als onveilig is geclassificeerd, wordt de website geblokkeerd en wordt een waarschuwingspagina weergegeven in uw browser.

De pagina bevat informatie, zoals de URL van de website en de gedetecteerde bedreiging.

U moet beslissen wat u vervolgens wilt doen. De volgende opties zijn beschikbaar:

- Verlaat de website door te klikken op **BRENG ME TERUG NAAR EEN VEILIGE LOCATIE**.
- Ga ondanks de waarschuwing door met uw bezoek aan de website, door te klikken op **Ik begrijp de risico's; breng me toch naar de webpagina**.
- Als u zeker bent dat de gedetecteerde website veilig is, klikt u op **INDIENEN** om deze toe te voegen aan de uitzonderingen. We raden aan dat u enkel websites toevoegt die u volledig vertrouwt.

16. KWETSBAARHEID

Een belangrijke stap bij het beschermen van uw apparaat tegen kwaadwillende acties en applicaties is het up-to-date houden van het besturingssysteem en van de applicaties die u regelmatig gebruikt. Bovendien: om ongeoorloofde fysieke toegang tot uw apparaat te voorkomen, moeten sterke wachtwoorden (wachtwoorden die niet makkelijk kunnen geraden worden) geconfigureerd worden voor elke Windows-gebruikersaccount en voor de Wi-Fi-netwerken waarmee u een verbinding maakt.

Bitdefender biedt twee eenvoudige manieren om de kwetsbaarheden van uw systeem op te lossen:

- U kunt uw systeem scannen op kwetsbaarheden en ze stapsgewijs repareren met de optie **Kwetsbaarheidscan**.
- Met de automatische kwetsbaarheidsbewaking kunt u de gedetecteerde kwetsbaarheden controleren en oplossen in het venster Kennisgevingen.

Het is aanbevolen de systeemkwetsbaarheden om de week of twee weken te controleren en op te lossen.

16.1. Uw systeem scannen op kwetsbaarheden

Om kwetsbaarheden in het systeem te detecteren, vereist Bitdefender een actieve internetverbinding.

Om uw systeem op kwetsbaarheden te scannen:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Bescherming**.
2. In het deelvenster **KWETSBAARHEID** klikt u op **Openen**.
3. Op het tabblad **Kwetsbaarheidsscan** klikt u op **Scan starten**. Vervolgens wacht u tot Bitdefender uw systeem controleert op kwetsbaarheden. De gedetecteerde kwetsbaarheden worden gegroepeerd in drie categorieën:
   - **BESTURINGSSYSTEEM**
     - **Beveiliging Besturingssysteem**

       Gewijzigde systeeminstellingen die uw apparaat en gegevens zouden kunnen aantasten, zoals het niet weergeven van waarschuwingen wanneer uitgevoerde bestanden zonder uw toestemming wijzigingen uitvoeren op uw systeem, of wanneer MTP-apparaten zoals telefoons

of camera's verbinding maken en verschillende bewerkingen uitvoeren zonder uw medeweten.

- **Kritieke Windows updates**

  Er wordt een lijst weergegeven met kritieke Windows-updates die niet geïnstalleerd zijn op uw computer. Het is mogelijk dat u het systeem opnieuw moet opstarten, zodat Bitdefender de installatie kan voltooien. Het kan even duren voordat de updates geïnstalleerd zijn.

- **Zwakke Windows-accounts**

  U ziet de lijst van Windows gebruikersaccounts die zijn geconfigureerd op uw apparaat en de beschermingsniveaus van de wachtwoorden. U kunt kiezen om de gebruiker te vragen het wachtwoord te wijzigen bij de volgende aanmelding of u kunt het wachtwoord zelf onmiddellijk wijzigen. Om een nieuw wachtwoord in te stellen voor uw systeem, selecteert u **Wachtwoord nu wijzigen**.

  Om een sterk wachtwoord te maken, raden we aan dat u een combinatie gebruikt van hoofdletters en kleine letters, getallen en speciale tekens (zoals #, $ of @).

- **TOEPASSINGEN**
  - **Browserveiligheid**

    Wijziging in de instellingen van uw apparaat, waardoor bestanden en programma's die zijn gedownload via Internet Explorer zonder integriteitsvalidering kunnen worden uitgevoerd. Dit kan ervoor zorgen dat uw apparaat wordt aangetast.

  - **Toepassings-updates**

    Om informatie te zien over de toepassing die moet worden bijgewerkt, klikt u erop in de lijst.

    Als een toepassing niet up-to-date is, klikt u op **NIEUWE VERSIE DOWNLOADEN** om de laatste versie te downloaden.

- **NETWERK**
  - **Netwerk en identificatiegegevens**

    Gewijzigde systeeminstellingen zoals het automatisch verbinden met open hotspot-netwerken zonder uw medeweten of het niet afdwingen van versleuteling van uitgaand beveiligd verkeer.

- **Wifi-netwerken en routers**

  Om meer te weten over het draadloze netwerk en de router waarmee u verbinding hebt gemaakt, klikt u erop in de lijst. Als het aanbevolen wordt dat u voor uw thuisnetwerk een sterker wachtwoord kiest, zorg dan dat u onze instructies volgt, zodat u verbonden kunt blijven zonder dat u zich zorgen hoeft te maken over uw privacy.

  Wanneer andere aanbevelingen beschikbaar zijn, volt u de instructies zodat u zeker bent dat uw thuisnetwerk veilig blijft tegen de indiscrete blikken van hackers.

16.2. De automatische kwetsbaarheidsbewaking gebruiken

Bitdefender scant uw systeem regelmatig op de achtergrond op kwetsbaarheden en houdt gegevens bij van de gevonden problemen in het venster Kennisgevingen.

Zo kunt u de opgespoorde problemen controleren en verhelpen:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Notificaties**.
2. In het tabblad **Alle** selecteert u de kennisgeving betreffende de Kwetsbaarheidsscan.
3. U kunt gedetailleerde informatie betreffende de gedetecteerde kwetsbaarheden van het systeem zien. Afhankelijk van het probleem, gaat u als volgt te werk om een specifieke kwetsbaarheid te herstellen:
   - Klik op **Installeren** als er Windows-updates beschikbaar zijn.
   - Indien automatische Windows Update geïnactiveerd is klikt u op **Activeren**.
   - Als een toepassing verouderd is, klikt u op **Nu updaten** om een link te zoeken naar de webpagina van de verkoper, vanaf waar u de nieuwste versie van die toepassing kunt installeren.
   - Als een Windows-gebruikersaccount een zwak wachtwoord heeft, klikt u op **Wachtwoord veranderen** om de gebruiker te forceren het wachtwoord te wijzigen bij de volgende aanmelding of wijzigt u zelf het wachtwoord. Voor een sterk wachtwoord gebruikt u een combinatie van hoofdletters en kleine letters, getallen en speciale tekens (zoals #, $ of @).

- Als de Windows-functie Autorun is ingeschakeld, klikt u op **Verhelpen** om de functie uit te schakelen.
- Indien de router die u hebt geconfigureerd een zwak wachtwoord heeft ingesteld, klikt u op **Wachtwoord wijzigen** om naar de interface te gaan, waar u een sterk wachtwoord kunt instellen.
- Klik op **Wifi-instellingen wijzigen** indien het netwerk waarmee u verbonden bent, kwetsbaarheden heeft die uw systeem in gevaar kunnen brengen.

De controle-instellingen voor kwetsbaarheid configureren:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Bescherming**.
2. In het deelvenster **KWETSBAARHEID** klikt u op **Openen**.

> **Belangrijk**
> Om automatisch op de hoogte te worden gebracht over kwetsbaarheden van het systeem of de toepassing, moet u de optie **Kwetsbaarheid** ingeschakeld houden.

3. Ga naar het tabblad **INSTELLINGEN**
4. Kies de systeemkwetsbaarheden die u regelmatig wilt controleren met de overeenkomende schakelaars.

Windows updates
Controleer of uw Windows-besturingssysteem over de laatste kritieke beveiligingsupdates van Microsoft beschikt.

Toepassings-updates
Controleer of toepassingen geïnstalleerd op uw systeem up-to-date zijn. Verouderde toepassingen kunnen door kwaadaardige software worden misbruikt, waardoor uw PC kwetsbaar wordt voor aanvallen van buitenaf.

Gebruikerswachtwoorden
Controleer of de wachtwoorden van de Windows-accounts en routers die op het systeem zijn geconfigureerd, gemakkelijk te raden zijn. Het instellen van moeilijk te raden wachtwoorden (sterke wachtwoorden) maakt het bijzonder moeilijk voor hackers om in uw systeem in te breken. Een sterk wachtwoord bevat hoofdletters en kleine letters, cijfers en speciale tekens (zoals #, $ of @).

Autoplay

Controleer de status van de Windows-functie Autorun. Met deze functie kunnen toepassingen automatisch worden gestart vanaf cd's, dvd,'s, USB-stations of andere externe apparaten.

Sommige types bedreigingen gebruiken Autorun om zich automatisch te verspreiden van de verwisselbare media naar de PC. Daarom is het aanbevolen deze Windows-functie uit te schakelen.

Wi-Fi Security Advisor

Controleer of het draadloze thuisnetwerk waarmee u verbonden bent al dan niet veilig is en of er kwetsbaarheden zijn. Controleer ook of het wachtwoord van uw thuisrouter sterk genoeg is en hoe u het veiliger kunt maken.

De meeste onbeveiligde draadloze netwerken zijn niet veilig, waardoor de indiscrete ogen van hackers toegang krijgen tot uw persoonlijke activiteiten.

Opmerking

Als u de bewaking van een specifieke kwetsbaarheid uitschakelt, worden verwante problemen niet langer opgenomen in het venster Kennisgevingen.

16.3. Wi-Fi Security Advisor

Als u onderweg bent, in een coffee shop gaat werken of in de luchthaven wacht, kan het de snelste oplossing zijn om een verbinding te maken met een openbaar draadloos netwerk om betalingen te doen, e-mails te lezen of sociale netwerkaccounts te raadplegen. Maar er kunnen nieuwsgierige ogen zijn, die uw persoonlijke gegevens proberen te stelen en kijken hoe de informatie door het netwerk heen druppelt.

Persoonlijke gegevens zijn de wachtwoorden en gebruikersnamen die u gebruikt om naar uw online accounts te gaan, zoals e-mails, bankrekeningen, sociale media-accounts, maar ook de berichten die u verzendt.

Gewoonlijk zijn openbare draadloze netwerken niet veilig, aangezien ze geen wachtwoord vragen om u aan te melden, en als dat wel het geval is, kan het wachtwoord ter beschikking gesteld worden van iedereen die een verbinding wil maken. Bovendien kunnen er kwaadaardige of honingpotnetwerken zijn, die een doelwit vormen voor cybercriminelen.

Om u te beschermen tegen de gevaren van onveilige of onversleutelde openbare draadloze hotspots, analyseert Bitdefender Wi-Fi Security Advisor hoe veilig een draadloos netwerk is, en indien nodig beveelt hij u aan om Bitdefender VPN te gebruiken.

De Bitdefender Wi-Fi Security Advisor geeft u informatie over:

- Thuis-Wi-Fi-netwerken
- Wifinetwerken op kantoor
- Openbare Wi-Fi-netwerken

16.3.1. De meldingen van Wi-Fi Security Advisor aan- of uitzetten

Om de meldingen van Wi-Fi Security Advisor aan of uit te zetten:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Bescherming**.
2. In het deelvenster **KWETSBAARHEID** klikt u op **Openen**.
3. Ga naar het venster **Instellingen** en schakel de optie **Wifi Beveiligingsadviseur** in of uit.

16.3.2. Thuis-Wi-Fi-netwerk configureren

Uw thuisnetwerk beginnen configureren:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Bescherming**.
2. In het deelvenster **KWETSBAARHEID** klikt u op **Openen**.
3. Ga naar het venster **Wifi Beveiligingsadviseur** en klik op **Wifi thuis**.
4. Klik in het tabblad **Thuis-wifi** op **THUIS-WIFI SELECTEREN**.

   Er wordt een lijst weergegeven met de draadloze netwerken waarmee u tot nu toe een verbinding hebt gemaakt.
5. Duid uw thuisnetwerk aan en klik daarna op **SELECTEREN**.

Indien een thuisnetwerk als onbeveiligd of onveilig wordt beschouwd, worden configuratieaanbevelingen weergegeven om de beveiliging te verbeteren.

Om het draadloze netwerk dat u als thuisnetwerk hebt ingesteld, te verwijderen, klikt u op de knop **VERWIJDEREN**.

Om een nieuw draadloos netwerk als thuis-wifi toe te voegen, klikt u op **Nieuwe thuis-wifi selecteren**.

16.3.3. Wifinetwerk op kantoor configureren

Om uw kantoornetwerk te configureren:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Bescherming**.
2. In het deelvenster **KWETSBAARHEID** klikt u op **Openen**.
3. Ga naar het venster **Wifi Beveiligingsadviseur** en klik op **Wifi kantoor**.
4. Klik in het tabblad **Kantoor-wifi** op **KANTOOR-WIFI SELECTEREN**.

   Er wordt een lijst weergegeven met de draadloze netwerken waarmee u tot nu toe een verbinding hebt gemaakt.
5. Duid het netwerk van uw kantoor aan en klik op **SELECTEREN**.

Indien een netwerk voor kantoor als onbeveiligd of onveilig wordt beschouwd, worden configuratieaanbevelingen weergegeven om de beveiliging ervan te verbeteren.

Om het draadloze netwerk dat u als netwerk voor kantoor hebt ingesteld, te verwijderen, klikt u op **VERWIJDEREN**.

Om een nieuw draadloos netwerk als kantoor-wifi toe te voegen, klikt u op **Nieuwe kantoor-wifi selecteren**.

16.3.4. Openbare Wifi

Terwijl u met een onbeveiligd of onveilig draadloos netwerk verbonden bent, wordt het openbare Wi-Fi-profiel geactiveerd. Terwijl u in dit profiel werkt, is Bitdefender Antivirus Plus ingesteld om automatisch de volgende programma-instellingen uit te voeren:

- Advanced Threat Defense is ingeschakeld
- De volgende instellingen van Online Threat Prevention zijn ingeschakeld:
  - Versleutelde webscan
  - Bescherming tegen fraude
  - Bescherming tegen phishing

- Er is een knop beschikbaar die Bitdefender Safepay™ opent. In dit geval is de Hotspot-bescherming voor onbeveiligde netwerken standaard geactiveerd.

16.3.5. Informatie controleren over Wi-Fi-netwerken

Om informatie te controleren over de draadloze netwerken, verbindt u zich gewoonlijk met:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Bescherming**.
2. In het deelvenster **KWETSBAARHEID** klikt u op **Openen**.
3. Ga naar het venster **Wifi Beveiligingsadviseur**.
4. Afhankelijk van de informatie die u nodig hebt, selecteert u een van de drie tabbladen, **Thuis-wifi**, **Kantoor-wifi** of **Openbare wifi**.
5. Klik op **Details bekijken** naast het netwerk waar u meer informatie over wenst.

Er zijn drie types draadloze netwerken gefilterd naargelang belang. Elk type wordt aangeduid door een specifiek pictogram:

Wi-Fi is onveilig - betekent dat het beveiligingsniveau van het netwerk laag is. Dit betekent dat er een hoog risico bestaat als u het gebruikt en het is niet aanbevolen om betalingen uit te voeren of bankrekeningen te controleren zonder extra bescherming. In dergelijke situaties bevelen wij u aan om Bitdefender Safepay™ met Hotspot-bescherming voor onveilige netwerken geactiveerd.

Wi-Fi is niet veilig - betekent dat het beveiligingsniveau van het netwerk matig is. Dit betekent dat het kwetsbaarheden kan bevatten en het is niet aanbevolen om betalingen uit te voeren of bankrekeningen te controleren zonder extra bescherming. In dergelijke situaties bevelen wij u aan om Bitdefender Safepay™ met Hotspot-bescherming voor onveilige netwerken geactiveerd.

Wi-Fi is veilig - betekent dat het netwerk dat u gebruikt, veilig is. In dit geval kunt gevoelige gegevens gebruiken om online bewerkingen uit te voeren.

Als u op de koppeling **Informatie bekijken** in het gebied van elk netwerk klikt, worden de volgende gegevens weergegeven:

- **Beveiligd** - hier kunt u bekijken of het geselecteerde netwerk al dan niet beveiligd is. Onbeveiligde netwerken kunnen de gegevens die u gebruikt, toegankelijk laten.
- **Type versleuteling** - hier kunt u bekijken welk type versleuteling wordt gebruikt door het geselecteerde netwerk. Bepaalde versleutelingstypes zijn mogelijk niet veilig. Daarom bevelen we u sterk aan om informatie over het weergegeven versleutelingstype te controleren, zodat u zeker bent dat u beschermd bent terwijl u op het internet surft.
- **Kanaal/Frequentie** - hier kunt u de frequentie van het kanaal bekijken dat het geselecteerde netwerk gebruikt.
- **Wachtwoordkwaliteit** - hier kunt u bekijken hoe sterk het wachtwoord is. Merk op dat de netwerken met een zwak wachtwoord een doelwit vormen voor cybercriminelen.
- **Type aanmelding** - hier kunt u bekijken of het geselecteerde netwerk al dan niet beschermd is met een wachtwoord. Het is sterk aanbevolen om enkel een verbinding te maken met netwerken die een sterk wachtwoord hebben.
- **Type authentificatie** - hier kunt u bekijken welk type authentificatie wordt gebruikt door het geselecteerde netwerk.

17. RANSOMWARE-REMEDIËRING

Ransomware-remediëring van Bitdefender maakt een back-up van uw bestanden zoals documenten, afbeeldingen, video's of muziek, om te verzekeren dat ze worden beschermd tegen schade of verlies in geval van versleuteling door ransomware. Telkens een ransomware-aanval wordt gedetecteerd, blokkeert Bitdefender alle processen die in de aanval zijn betrokken en start het remediëringsproces op. Zo kunt u de inhoud van al uw bestanden herstellen, zonder het gevraagde losgeld te moeten betalen.

17.1. De Ransomware-remediëring in- of uitschakelen

Om de Ransomware-remediëring in of uit te schakelen:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Bescherming**.
2. Schakel de schakelaar in het paneel **RANSOMWARE-REMEDIËRING** in of uit.

> **Opmerking**
> Om te verzekeren dat uw bestanden tegen ransomware worden beschermd, raden we aan dat u Ransomware-remediëring ingeschakeld laat.

17.2. Automatisch herstellen in- of uitschakelen

Automatisch herstellen zorgt ervoor dat uw bestanden automatisch worden hersteld in geval van versleuteling door ransomware.

Om automatisch herstellen in of uit te schakelen:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Bescherming**.
2. Klik op **Beheren** in het deelvenster **RANSOMWARE-REMEDIËRING**.
3. In het venster Instellingen schakelt u de schakelaar voor **Automatisch herstellen** in of uit.

17.3. Bestanden bekijken die automatisch werden hersteld

Wanneer de optie **Automatisch herstellen** ingeschakeld is, herstelt Bitdefender automatisch de bestanden die door ransomware werden versleuteld. Zo kunt

u zorgeloos genieten van uw apparaat, want u weet dat uw bestanden veilig zijn.

Om bestanden te bekijken die automatisch werden hersteld:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Notificaties**.
2. In het tabblad **Alle** selecteert u de notificatie betreffende het ransomware-gedrag dat als laatste werd geremedieerd en klikt u op **Herstelde bestanden**.

   De lijst met herstelde bestanden wordt weergegeven. Hier kunt u ook de locatie waar uw bestanden werden hersteld, bekijken.

17.4. Versleutelde bestanden handmatig herstellen

Volg deze stappen indien u de bestanden die door ransomware werden versleuteld handmatig wilt herstellen:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Notificaties**.
2. In het tabblad **Alle** selecteert u de notificatie betreffende het ransomware-gedrag dat als laatste werd gedetecteerd en klikt u op **Versleutelde bestanden**.
3. De lijst met versleutelde bestanden wordt weergegeven.

   Klik op **Bestanden herstellen** om verder te gaan.
4. Indien een deel van of het gehele herstelproces mislukt, moet u de locatie kiezen waar de ontcijferde bestanden moeten worden bewaard. Klik op **LOCATIE VOOR HET HERSTEL** en kies een locatie op uw pc.
5. Er wordt een bevestigingsvenster weergegeven.

   Klik op **VOLTOOIEN** om het herstelproces te beëindigen.

Bestanden met de onderstaande extensies kunnen worden hersteld, indien ze worden versleuteld:

.3g2; .3gp; .7z; .ai; .aif; .arj; .asp; .aspx; .avi; .bat; .bin; .bmp; .c; .cda; .cgi; .class; .com; .cpp; .cs; .css; .csv; .dat; .db; .dbf; .deb;.doc; .docx; .gif; .gz; .h264; .h; .flv; .htm; .html;.ico; .jar; .java; .jpeg; .jpg;.js; .jsp; .key; .m4v; .mdb; .mid; .midi; .mkv; .mp3; .mp4; .mov; .mpg; .mpeg; .ods; .odp;.odt; .ogg; .pdf; .pkg; .php; .pl; .png; .pps; .ppt; .pptx; .ps; .psd; .py; .rar; .rm; .rtf; .sav; .sql; .sh; .svg; .swift; .swf; .tar; .tex; .tif; .tiff; .txt; .xlr; .xls; .xlsx; .xml; .wmv; .vb; .vob; .wav; .wks; .wma; .wpl; .wps; .wpd; .wsf; .z; .zip;

17.5. Toepassingen aan uitzonderingen toevoegen

U kunt de uitzonderingsregels voor vertrouwde toepassingen configureren zodat de functie Ransomware-remediëring deze niet blokkeert wanneer ze handelingen uitvoeren die op ransomware lijken.

Om toepassingen toe te voegen aan de uitzonderingenlijst van Ransomware-remediëring:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Bescherming**.
2. Klik op **Beheren** in het deelvenster **RANSOMWARE-REMEDIËRING**.
3. Ga naar het venster **Uitzonderingen** en klik op **+Een uitzondering toevoegen**.

18. BEVEILIGING WACHTWOORDBEHEERDER VOOR UW GEGEVENS

We gebruiken onze apparaaten om online te winkelen of onze rekeningen te betalen, om in te loggen op platforms van sociale media of op toepassingen voor instant messaging.

Maar zoals iedereen weet, is het niet altijd gemakkelijk om het wachtwoord te onthouden!

En we zijn niet voorzichtig als we online surfen, onze persoonlijke gegevens, zoals ons e-mailadres, onze ID van instant messaging of onze creditcardgegevens kunnen in gevaar komen.

Het bewaren van uw wachtwoorden of uw persoonlijke gegevens of een vel papier of in de computer kan gevaarlijk zijn, want ze kunnen worden gezien en gebruikt door mensen die deze gegevens willen stelen en gebruiken. En elk wachtwoord dat u hebt ingesteld voor uw online accounts of voor uw favoriete websites onthouden, is geen gemakkelijke taak.

Is er daarom een manier om ervan verzekerd te zijn dat we onze wachtwoorden vinden wanneer we ze nodig hebben? En kunnen we verzekerd blijven dat onze geheime wachtwoorden altijd veilig zijn?

Wachtwoordbeheerder helpt om uw wachtwoorden bij te houden, beveilgt uw privacy en bezorgt een veilige online surfervaring.

Door het gebruik van een enkel masterwachtwoord om naar uw gegevens te gaan, maakt Wachtwoordbeheerder het gemakkelijk voor u om uw wachtwoorden veilig te houden in een Portefeuille.

Om de beste beveiliging voor uw online activiteiten te bieden, is Wachtwoordbeheerder geïntegreerd met Bitdefender Safepay™ en verschaft een samengebundelde oplossing voor de verschillende wegen waarop uw persoonlijke gegevens in gevaar kunnen komen.

Wachtwoordbeheerder beveiligt de volgende persoonlijke gegevens:

- Persoonlijke gegevens, zoals het e-mailadres of het telefoonnummer
- Logingegevens voor de websites
- Bankrekeninggegevens of het creditcardnummer
- Toegangsgegevens naar de e-mailaccounts

- Wachtwoorden voor de toepassingen
- Wachtwoorden voor de Wi-Fi-netwerken

18.1. Maak een nieuwe Portefeuilledatabase aan

Bitdefender-portefeuille is de plek waar u uw persoonlijke gegevens kunt opslaan. Voor een makkelijkere browserervaring moet u een als volgt een Portefeuilledatabase aanleggen:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Privacy**.
2. Klik in het venster **WACHTWOORDBEHEERDER** op **Instellingen**.
3. Klik in het venster **Mijn portefeuilles** op **Portefeuille toevoegen**.
4. Klik op **Aanmaken**.
5. Typ de vereiste informatie in de overeenkomende velden.
   - Portefeuillenaam - tik een unieke naam in voor de database van uw Portefeuille.
   - Masterwachtwoord - tik een wachtwoord in voor uw Portefeuille.
   - Hint - tik een hint in om het wachtwoord te herinneren.
6. Klik op **Doorgaan**.
7. Bij deze stap kunt u kiezen of uw informatie in de cloud wordt bewaard, door de schakelaar naast **Synchroniseren voor al mijn apparaten** te activeren. Kies de gewenste optie en klik daarna op **Verdergaan**.
8. Selecteer de webbrowser waarvan u de gegevens van wilt importeren.
9. Klik op **Voltooien**.

18.2. Importeer een bestaande database

Om een plaatselijk opgeslagen database te importeren:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Privacy**.
2. Klik in het venster **WACHTWOORDBEHEERDER** op **Instellingen**.
3. Klik in het venster **Mijn portefeuilles** op **Portefeuille toevoegen**.
4. Klik op **Een bestaande database importeren**.
5. Ga op uw apparaat naar de locatie waar u de Portefeuilledatabase hebt opgeslagen en selecteer het.

6. Klik op **Openen**.
7. Geef uw Portefeuille een naam en voer het wachtwoord dat bij de aanmaak werd toegekend, in.
8. Klik op **Importeren**.
9. Selecteer de programma's van waaruit u de Portefeuille legitimatiebewijzen wenst te laten importeren, en klik dan op de knop **Voltooien**.

18.3. De Portefeuille-database exporteren

Uw Portefeuilledatabase exporteren:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Privacy**.
2. Klik in het venster **WACHTWOORDBEHEERDER** op **Instellingen**.
3. Ga naar het venster **Mijn portefeuilles**.
4. Klik op de ••• -icoon op de gewenste portefeuille en selecteer vervolgens **Exporteren**.
5. Ga naar de locatie op uw apparaat waar u de Portefeuilledatabase wenst op te slaan en kies er vervolgens een naam voor.
6. Klik op **Opslaan**.

> **Opmerking**
> De Portefeuille moet geopend zijn om de **Exporteren**-optie beschikbaar te maken.
> Indien de portefeuille die u moet exporteren, vergrendeld is, klikt u op **PORTEFEUILLE ACTIVEREN** en voert u het wachtwoord in dat werd aangemaakt van bij het begin.

18.4. Synchroniseer uw portefeuilles in de cloud

De portefeuillesynchronisatie in de cloud in- of uitschakelen:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Privacy**.
2. Klik in het venster **WACHTWOORDBEHEERDER** op **Instellingen**.
3. Ga naar het venster **Mijn portefeuilles**.

4. Klik op de ••• -icoon op de gewenste portefeuille en selecteer vervolgens **Instellingen**.
5. Kies de gewenste optie in het venster dat verschijnt en klik vervolgens op **Opslaan**.

> **Opmerking**
> De Portefeuille moet geopend zijn om de **Exporteren**-optie beschikbaar te maken.
> Indien de portefeuille die u moet synchroniseren, vergrendeld is, klikt u op **PORTEFEUILLE ACTIVEREN** en voert u het wachtwoord in dat werd aangemaakt bij het begin.

18.5. Uw Portefeuille-gegevens beheren

Uw wachtwoorden beheren:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Privacy**.
2. Klik in het venster **WACHTWOORDBEHEERDER** op **Instellingen**.
3. Ga naar het venster **Mijn portefeuilles**.
4. Selecteer de gewenste Portefeuilledatabase en klik vervolgens op **PORTEFEUILLE ACTIVEREN**.
5. Voer het hoofdwachtwoord in en klik op **OK**.

Er verschijnt een nieuw venster. Selecteer de gewenste categorie in het bovenste deel van het venster:

- Identiteit
- Webpagina's
- Online bank
- E-mails
- Applicaties
- Wifi-netw.

De gegevens aanvullen / bewerken

- Om een nieuw wachtwoord toe te voegen, kiest u de gewenste categorie bovenaan en klikt u op **+ Item toevoegen**, vul de gegevens in de betreffende velden in en klik op de knop Opslaan.
- Om een gegeven in de tabel te bewerken, selecteert u het gegeven en klikt u rechts ernaast op de knop **Bewerken**.
- Om een invoer te verwijderen, selecteert u deze en klikt u op de knop **Verwijderen**.

18.6. De Wachtwoordbeheerderbeveiliging in- of uitschakelen

De bescherming van Wachtwoordmanager in- of uitschakelen:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Privacy**.
2. Schakel de schakelaar in het venster **WACHTWOORDBEHEERDER** in of uit.

18.7. De instellingen voor Wachtwoordbeheerder beheren

Het hoofdwachtwoord in detail configureren:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Privacy**.
2. Klik in het venster **WACHTWOORDBEHEERDER** op **Instellingen**.
3. Ga naar het venster **Instellingen**.

In de sectie **Beveiligingsinstellingen** zijn de volgende opties beschikbaar:

- **Mijn masterwachtwoord vragen wanneer ik inlog op mijn apparaat** - u wordt gevraagd uw masterwachtwoord in te voeren wanneer u toegang zoekt tot het apparaat.
- **Mijn masterwachtwoord vragen wanneer ik mijn browsers en toepassingen open** - u wordt gevraagd uw masterwachtwoord in te voeren wanneer u toegang zoekt tot een browser of toepassing.
- **Mijn masterwachtwoord niet vragen** - u wordt niet gevraagd uw masterwachtwoord in te voeren wanneer u toegang zoekt tot de apparaat, een browser of een toepassing.

- **Portefeuille automatisch vergrendelen wanneer ik mijn apparaat onbewaakt laat** - u wordt gevraagd uw masterwachtwoord in te voeren wanneer u na 15 minuten terugkeert naar uw apparaat.

Belangrijk
Zorg dat u uw masterwachtwoord onthoudt of bewaar het op een veilige plaats. Als u het wachtwoord vergeten bent, moet u het programma opnieuw installeren of contact opnemen met Bitdefender voor ondersteuning.

Verbeter uw ervaring

Om de browsers of toepassingen waarin u de wachtwoordmanager wilt integreren te selecteren:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Privacy**.
2. Klik in het venster **WACHTWOORDBEHEERDER** op **Instellingen**.
3. Selecteer het venster **Instellingen**.

   Schakel de schakelaar naast een app in om Wachtwoordbeheerder te gebruiken en uw ervaring te verbeteren:

   - Internet Explorer
   - Mozilla Firefox
   - Google Chrome
   - Safepay

Autofill configureren

De functie Autofill maakt het u gemakkelijk om verbinding te maken met uw favoriete websites of om in te loggen op uw online accounts. De eerste keer dat u uw certificaten en persoonlijke gegevens invoert in uw webbrowser, worden ze automatisch beveiligd in de Portefeuille.

Om de **Autofill**-instellingen te configureren:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Privacy**.
2. Klik in het venster **WACHTWOORDBEHEERDER** op **Instellingen**.
3. In het venster **Instellingen** scrolt u naar het tabblad **Autofill-instellingen**.
4. De volgende opties configureren:

   - **Configureren hoe Wachtwoordbeheerder uw gegevens beveiligt.**:

- **Inloggegevens automatisch opslaan in Portefeuille** - de logingegevens en andere herkenbare gegevens zoals uw persoonlijke en creditcardgegevens worden automatisch opgeslagen en bijgewerkt in de Portefeuille.
- **Vraag me elke keer** - u wordt elke keer gevraagd of u uw gegevens aan de Portefeuille wilt toevoegen.
- **Niet opslaan, ik werk de gegevens handmatig bij** - de gegevens kunnen alleen handmatig aan de Portefeuille worden toegevoegd.

- **Inlogreferenties automatisch aanvullen**:
  - **Autofill logingegevens elke keer** - de gegevens worden automatisch in de browser ingevuld.
- **Autofill formulieren**:
  - **Geef mijn in te vullen opties aan als ik een pagina met formulieren bezoek** - een pop-up met de invulopties verschijnt telkens wanneer Bitdefender detecteert dat u een online betaling wilt uitvoeren of wilt intekenen.

De Wachtwoordbeheerder beheren vanuit uw browser

U kunt de informatie Wachtwoordbeheerder gemakkelijk beheren vanuit uw browser, zodat u alle belangrijke gegevens bij de hand hebt. De invoegtoepassing Bitdefender wordt ondersteund door de volgende browsers: Google Chrome, Internet Explorer en Mozilla Firefox, en hij is ook geïntegreerd in Safepay.

Om naar de Portefeuille-extensie van Bitdefender te gaan, opent u uw webbrowser, accepteert de installatie van de invoegtoepassing en klikt op het pictogram op de taakbalk.

De Portefeuille-extensie van Bitdefender bevat de volgende opties:

- Portefeuille openen - opent de Portefeuille.
- Portefeuille vergrendelen - vergrendelt de portefeuille.
- Webpagina's - opent een submenu met alle log-ins van websites die in Portefeuille zijn bewaard. Klik op **Webpagina toevoegen** om de nieuwe websites aan de lijst toe te voegen.

- Formulieren invullen - opent een submenu met de gegevens die u voor een speciale categorie hebt toegevoegd. Van hieruit kunt u nieuwe gegevens aan uw Portefeuille toevoegen.
- Wachtwoordgenerator - hiermee kunt u willekeurige wachtwoorden genereren die u voor nieuwe of bestaande accounts kunt gebruiken. Klik op **Geavanceerde instellingen tonen** om de complexiteit van het wachtwoord aan te passen.
- Instellingen - opent het instellingenvenster van Wachtwoordbeheerder.
- Probleem melden - meldt elk willekeurig probleem dat u ondervindt met Wachtwoordbeheerder van Bitdefender

19. ANTI-TRACKER

Vele websites die u bezoekt, gebruiken trackers om informatie te verzamelen over uw gedrag. Ze kunnen deze informatie vervolgens delen met derden of ze kunnen de informatie gebruiken om u advertenties te laten zien die voor u relevanter zijn. Eigenaars van websites verdienen zo geld, om u gratis inhoud te kunnen bieden of om draaiende te blijven. Naast het verzamelen van informatie, kunnen trackers uw surfervaring vertragen of uw bandbreedte opgebruiken.

Als de extensie Anti-tracker van Bitdefender geactiveerd is in uw webbrowser, vermijdt u deze tracking, zorgt u dat uw gegevens privé blijven terwijl u online surft en wordt de laadtijd voor websites versneld.

De Bitdefender-extensie is compatibel met de volgende webbrowsers:

- Internet Explorer
- Google Chrome
- Mozilla Firefox

De trackers die we detecteren worden in de volgende categorieën gegroepeerd:

- **Reclame** - wordt gebruikt voor de analyse van patronen in websiteverkeer, het gedrag van gebruikers of het verkeer van bezoekers.
- **Klanteninteractie** - wordt gebruikt om de interactie van gebruikers met verschillende invoervormen, zoals chat of ondersteuning, te meten.
- **Essentieel** - wordt gebruikt om de kritieke functionaliteiten van webpagina's te monitoren.
- **Website-analytics** - wordt gebruikt om gegevens over het gebruik van webpagina's te verzamelen.
- **Sociale Media** - wordt gebruikt voor de monitoring van het sociale publiek, de activiteiten en het gebruikersengagement met verschillende sociale mediaplatformen.

19.1. Interface van Anti-tracker

Wanneer de extensie Anti-tracker van Bitdefender geactiveerd is, verschijnt het pictogram naast de zoekbalk in uw webbrowser. Telkens u een

website bezoekt, ziet u een teller op het pictogram: dat getal verwijst naar de gedetecteerde en geblokkeerde trackers. Voor meer details over de geblokkeerde trackers, klikt u op het pictogram om de interface te openen. U ziet, naast het aantal geblokkeerde trackers, ook hoeveel tijd de pagina nodig heeft om te laden alsook de categorieën waartoe de gedetecteerde trackers behoren. Om een lijst weer te geven van de websites die aan tracking doen, klikt u op de gewenste categorie.

Om de blokkering van trackers door Bitdefender op te heffen voor de website die u momenteel bezoekt, klikt u op **Bescherming op deze website pauzeren**. Deze instelling is enkel van toepassing zolang u de website open hebt staan en gaat terug naar zijn initiële staat zodra u de website verlaat.

Om toe te staan dat trackers van een specifieke categorie uw activiteiten volgen, klikt u op de gewenste activiteit en vervolgens op de bijhorende knop. Indien u zich bedenkt, klikt opnieuw op dezelfde knop.

19.2. Anti-tracker van Bitdefender uitschakelen

Om de Anti-tracker van Bitdefender uit te schakelen:

- Vanuit uw webbrowser:
  1. Open uw webbrowser.
  2. Klik op het pictogram naast de adresbalk in uw webbrowser.
  3. Klik op het pictogram in de rechterbovenhoek.
  4. Gebruik de bijhorende schakelaar om uit te schakelen.

     Het pictogram voor Bitdefender wordt grijs.
- Van de Bitdefender-interface:
  1. Klik in het navigatiemenu in de Bitdefender-interface op **Privacy**.
  2. Klik in het **ANTI-TRACKER** paneel op **Instellingen**.
  3. Schakel de overeenstemmende schakelaar uit naast de webbrowser waarvoor u de extensie wenst uit te schakelen.

19.3. Toestaan dat een website aan tracking doet

Wilt u dat tracking wordt toegepast wanneer u een bepaalde website bezoekt, kunt u dit adres als volgt toevoegen aan de uitzonderingen:

1. Open uw webbrowser.
2. Klik op het pictogram  naast de zoekbalk.
3. Klik op het pictogram  in de rechterbovenhoek.
4. Bent u op de website die u wilt toevoegen aan de uitzonderingen, klikt u op **Huidige website aan lijst toevoegen**.

   Wilt u een andere website toevoegen, voert u het adres in het bijhorende veld in en klikt u op  .

20. VPN

De VPN-app kan worden geïnstalleerd vanaf uw Bitdefender-product en kan op elk ogenblik worden gebruikt om een extra beschermingslaag toe te voegen aan uw verbinding. De VPN werkt zoals een tunnel tussen uw apparaat en het netwerk waarmee u verbindt: de VPN beveiligt die verbinding, door aan de hand van versleuteling volgens bankrichtlijnen de gegevens te versleutelen en door uw IP-adres te verbergen, waar u ook bent. Uw dataverkeer wordt omgeleid via een andere server, waardoor het praktisch onmogelijk wordt om uw apparaat te identificeren tussen de talloze andere toestellen die gebruikmaken van onze diensten. Wanneer u via Bitdefender VPN verbonden bent met het internet kunt u bovendien inhoud bekijken die normaal afgeschermd wordt in bepaalde gebieden.

Opmerking
Sommige landen hanteren internetcensuur. Het gebruik van VPN's is op hun grondgebied dan ook bij wet verboden. Om wettelijke gevolgen te vermijden, is het mogelijk dat er een waarschuwingsbericht verschijnt wanneer u de app Bitdefender VPN voor het eerst probeert te gebruiken. Door het gebruik van de app verder te zetten, bevestigt u dat u op de hoogte bent van de toepasselijke reguleringen van het land en van de risico's die u mogelijk loopt.

20.1. VPN Openen

Volg een van de volgende methoden om naar de hoofdinterface van Bitdefender VPN te gaan:

- Vanuit het systeemvak
  1. Rechtsklik op het icoon in het systeemvak en klik vervolgens op **Tonen**.
- Van de Bitdefender-interface:
  1. Klik in het navigatiemenu in de Bitdefender-interface op **Privacy**.
  2. Klik op **VPN openen** in het venster **VPN**.

20.2. VPN-interface

De VPN-interface geeft de status van de app weer: verbonden of niet verbonden. Voor gebruikers met de gratis versie stelt Bitdefender de serverlocatie automatisch in op de meest geschikte server.

Premium-gebruikers hebben de mogelijkheid de serverlocatie waarmee ze wensen te verbinden, te wijzigen. Voor meer informatie over VPN-abonnementen, raadpleeg "*Abonnementen*" (p. 126).

Om te verbinden of om de verbinding te verbreken: klik op de status die bovenaan het scherm wordt weergeven of rechtsklik op het icoon systeemvak. Het icoon systeemvak geeft een groen vinkje weer wanneer de VPN verbonden is, en een rood vinkje wanneer de verbinding verbroken is.

Tijdens de verbinding worden de verstreken tijd en de gebruikte bandbreedte weergegeven op het onderste gedeelte van de interface.

Om het gehele gebied **Menu** te zien, klikt u aan de linkerbovenzijde op het pictogram ☰. U hebt hier de volgende opties:

- **Mijn Account** – geeft details weer over uw Bitdefender-account en VPN-abonnement. Klik op **Account Wisselen** indien u met een andere account wenst in te loggen.

  Klik op **Hier toevoegen** om een activeringscode voor Bitdefender Premium VPN toe te voegen.

- **Instellingen** – u kunt het gedrag van uw product aanpassen naargelang uw noden. De instellingen zijn gegroepeerd in twee categorieën:

  - **Algemeen**
    - Notificaties
    - Opstarten - kies of Bitdefender VPN bij het opstarten wordt uitgevoerd of niet
    - Productrapporten - dien anonieme productrapporten in om ons te helpen uw ervaring te verbeteren
    - Donkere modus
    - Taal
  - **Geavanceerd**
    - Internet Kill-Switch - deze voorziening onderbreekt tijdelijk al het internetverkeer indien de VPN-verbinding onbedoeld wordt verbroken. Zodra u terug online bent, wordt de verbinding opnieuw tot stand gebracht.

- Autoconnect - Verbind Bitdefender VPN automatisch wanneer u een openbaar of niet-beveiligd wifinetwerk gebruikt of wanneer een app voor peer-to-peer-bestandsuitwisseling wordt gestart

- **Ondersteuning** - u hebt toegang tot ons platform Ondersteuningscentrum, waar u artikels kunt lezen over hoe u Bitdefender VPN gebruikt of over hoe u ons feedback kunt sturen.

- **Over deze versie** - informatie over de geïnstalleerde versie.

20.3. Abonnementen

Bitdefender VPN biedt dagelijks gratis 200 MB dataverkeer per apparaat om uw verbinding te beveiligen telkens u dit nodig hebt, en verbindt bovendien automatisch met de beste serverlocatie.

Upgrade naar de premium-versie voor onbeperkt dataverkeer en toegang tot afgeschermde inhoud overal ter wereld, doordat u de serverlocatie naar wens kunt selecteren.

U kunt op elk ogenblik upgraden naar de Bitdefender Premium VPN-versie door te klikken op de knop **Upgraden** in de productinterface.

Het Bitdefender Premium VPN-abonnement is onafhankelijk van het abonnement voor Bitdefender Antivirus Plus: u kunt het dus gedurende de hele geldigheid ervan gebruiken, ongeacht de status van het abonnement van de beveiligingsoplossing. Indien het Bitdefender Premium VPN-abonnement vervalt, maar indien het abonnement voor Bitdefender Antivirus Plus nog actief is, gaat u terug naar de gratis versie.

Bitdefender VPN is een cross-platform product, beschikbaar in Bitdefender-producten die compatibel zijn met Windows, macOS, Android en iOS. Eens u upgradet naar de premium-versie, kunt u uw abonnement op alle producten gebruiken, op voorwaarde dat u inlogt met dezelfde Bitdefender-account.

21. SAFEPAY BEVEILIGING VOOR ONLINE TRANSACTIES

De computer wordt in snel tempo het hoofdhulpmiddel voor winkelen en bankieren. Facturen betalen, geld overmaken, bijna alles wat u zich maar voor kunt stellen kopen, dat alles is nooit sneller en gemakkelijker geweest.

Dit houdt in het verzenden via Internet van persoonlijke gegevens, account- en creditcardgegevens, wachtwoorden en andere soorten privégegevens, met andere woorden, precies het soort gegevensstroom waar cybercriminelen graag gebruik van maken. Hackers zijn meedogenloos in hun pogingen deze gegevens te stelen, dus u kunt nooit voorzichtig genoeg zijn als het om het beveiligen van online transacties gaat.

Bitdefender Safepay™ is allereerst een beveiligde browser, een verzegelde omgeving, die is bestemd voor het privé en veilig houden van online bankieren, e-shopping en andere soorten online transacties.

Voor de beste privacybeveiliging is Bitdefender-Wachtwoordbeheerder geïntegreerd in Bitdefender Safepay™ om uw gegevens te beveiligen wanneer u naar persoonlijke online plaatsen gaat. Zie "*Beveiliging Wachtwoordbeheerder voor uw gegevens*" (p. 113) voor meer informatie.

Bitdefender Safepay™ biedt de volgende functies:

- Het blokkeert de toegang tot uw desktop en elke poging snapshots van uw scherm te maken.
- Het beveiligt uw geheime wachtwoorden als u online surft met Wachtwoordbeheerder.
- Het verschaft een virtueel toetsenbord dat het, als het wordt gebruikt, onmogelijk maakt voor hackers uw aanslagen te lezen.
- Het is volledig onafhankelijk van uw andere browsers.
- Het biedt een ingebouwde hotspotbeveiliging die kan worden gebruikt wanneer uw apparaat is verbonden met onbeveiligde Wi-Fi-netwerken.
- Het ondersteunt bookmarks en stelt u in staat om te surfen tussen uw favoriete bank/winkelsites.
- Het is niet beperkt tot bankieren en online winkelen. Elke website kan worden geopend in Bitdefender Safepay™.

21.1. Bitdefender Safepay™ gebruiken

Standaard detecteert Bitdefender wanneer u naar een online banksite of online winkel in een willekeurige browser op uw apparaat surft en het vraagt u deze site te starten in Bitdefender Safepay™.

Om naar de hoofdinterfae van Bitdefender Safepay™ te gaan, gebruikt u een van de volgende manieren:

- Vanuit de Bitdefender-interface:
  1. Klik in het navigatiemenu in de Bitdefender-interface op **Privacy**.
  2. Klik op **Instellingen** in het deelvenster **SAFEPAY**.
  3. In het venster **Safepay** klikt u op **Safepay starten**.
- Voor Windows:
  - In **Windows 7**:
    1. Klik op **Start** en ga naar **Alle Programma's**.
    2. Klik op **Bitdefender**.
    3. Klik op **Bitdefender Safepay™**.
  - In **Windows 8 en Windows 8.1**:

    Zoek Bitdefender Safepay™ vanuit het Windows-startscherm (u kunt bijvoorbeeld beginnen met het typen van "Bitdefender Safepay™", rechtstreeks in het startscherm) en klik op het pictogram.
  - In **Windows 10**:

    Typ "Bitdefender Safepay™" in het zoekveld in de taakbalk en klik op het pictogram ervan.

Indien u gewend bent aan webbrowsers, zult u geen moeite hebben Bitdefender Safepay™ te gebruiken - het ziet eruit en gedraagt zich als een gewone browser:

- geef de URL's op in de adresbalk van de sites waar u heen wilt gaan.
- voeg tabs toe om meerdere websites te bezoeken in het Bitdefender Safepay™-venster door te klikken op  .

- surf terug en vooruit en vernieuw pagina's met gebruikmaking van respectievelijk  .
- ga naar Bitdefender Safepay™ instellingen door te klikken op en kies **Instellingen**.
- beveilig uw wachtwoorden met Wachtwoordbeheerder door te klikken op  .
- beheer uw favorieten door te klikken op  naast de adresbalk.
- het virtuele toetsenbord openen door te klikken op  .
- vergroot of verklein de browserafmetingen door gelijktijdig te drukken op de toetsen **Ctrl** en **+/-** op het numerieke toetsenbord.
- informatie bekijken over uw Bitdefender-product door te klikken op en kies **Over...**.
- druk belangrijke informatie af door te klikken op en **Afdrukken** te kiezen.

Opmerking
Om tussen Bitdefender Safepay™ en Windows-bureaublad te wisselen, drukt u op de toetsen **Alt+Tab** of klikt u in de linkerbovenhoek van het venster op de optie **Wisselen naar Bureaublad**.

21.2. Instellingen configureren

Klik op en kies **Instellingen** om Bitdefender Safepay™ te configureren:

Regels voor Bitdefender Safepay toepassen voor domeinen die worden geopend

De websites die u hebt toegevoegd aan Bladwijzers met de optie **Automatisch openen in Safepay** ingeschakeld, verschijnen hier. Wilt u het automatisch openen met Bitdefender Safepay™ opheffen voor een

website uit de lijst, klikt u op × naast het gewenste item in de kolom **Verwijderen**.

Pop-ups blokkeren
U kunt ervoor kiezen om pop-ups te blokkeren door te klikken op de overeenkomende schakelaar.

U kunt ook een lijst aanmaken met websites waarvan u pop-ups toestaat. De lijst mag websites bevatten die u volledig vertrouwt.

Om een site toe te voegen aan de lijst, geeft u het adres van de site op in het overeenkomende veld en klikt u op **Domein toevoegen**.

Om een website uit de lijst te verwijderen, selecteert u het X-je bij het gewenste gegeven.

Plug-ins beheren
U kunt kiezen of u specifieke plug-ins in Bitdefender Safepay™ wenst te activeren of inactiveren.

Certificaten beheren
U kunt certificaten van uw systeem importeren naar een certificatenwinkel.

Klik op **IMPORTEREN** en volg de wizard om de certificaten te gebruiken in Bitdefender Safepay™.

Virtueel toetsenbord gebruiken
Het Virtuele toetsenbord verschijnt automatisch wanneer een wachtwoordveld wordt geselecteerd.

Gebruik de bijhorende schakelaar om de functie te activeren of inactiveren.

Bevestiging afdrukken
Activeer deze optie indien u uw bevestiging wenst te geven voordat het afdrukproces start.

21.3. Favorieten beheren

Indien u de automatische detectie van sommige of alle websites hebt uitgeschakeld, of Bitdefender detecteert bepaalde websites eenvoudigweg niet, dan kunt u favorieten toevoegen aan Bitdefender Safepay™ zodat u favoriete websites in de toekomst eenvoudig kunt starten.

Volg deze stappen om een URL toe te voegen aan Bitdefender Safepay™-favorieten:

1. Klik op ••• en kies **Favorieten** om de pagina Favorieten te openen.

   Opmerking
   De pagina met favorieten is standaard geopend als u Bitdefender Safepay™ start.

2. Klik op de knop **+** om een nieuwe favoriete pagina toe te voegen.
3. Geef de URL en de titel van de bladwijzer in en klik vervolgens op **AANMAKEN**. Vink de optie **Automatisch openen in Safepay** aan indien u de gemarkeerde pagina wilt openen met Bitdefender Safepay™, telkens als u er naartoe gaat. De URL wordt ook toegevoegd aan de Domeinenlijst op de instellingen-pagina.

21.4. Safepay-notificaties uitschakelen

Bitdefender-product is zo ingesteld dat u via een pop-up op de hoogte wordt gebracht wanneer een website voor internetbankieren wordt gedetecteerd.

Om Safepay-notificaties uit te schakelen:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Privacy**.
2. Klik op **Instellingen** in het deelvenster **SAFEPAY**.
3. In het venster **Instellingen** schakelt u de schakelaar naast **Safepay-notificaties** in.

21.5. VPN met Safepay gebruiken

Het Bitdefender-product kan zo worden ingesteld dat de VPN-app automatisch samen met Safepay wordt opgestart, zodat u uw online betalingen ook op netwerken die niet zijn beveiligd, in een veilige omgeving kunt uitvoeren.

Om de VPN-app samen met Safepay te gebruiken:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Privacy**.
2. Klik op **Instellingen** in het deelvenster **SAFEPAY**.
3. In het venster **Instellingen** schakelt u de schakelaar naast **VPN gebruiken met Safepay** in.

22. USB IMMUNIZER

De Autorun-functie die is ingebouwd in Windows-besturingssystemen is een heel handig hulpmiddel waardoor apparaten automatisch een bestand kunnen uitvoeren vanaf media die zijn verbonden met deze apparaten. Software-installaties bijvoorbeeld kunnen automatisch starten als er een cd in de cd-lezer wordt geschoven.

Helaas kan deze functie ook worden gebruikt door bedreigingen om automatisch te starten en zo in uw apparaat te infiltreren vanaf media die beschreven kunnen worden, zoals USB-sticks en geheugenkaarten die via kaartlezers worden verbonden. De afgelopen jaren zijn er talloze op Autorun gebaseerde aanvallen aangemaakt.

Met USB Immunizer kunt u voorkomen dat een willekeurige NTFS, FAT32 of FAT-geformatteerde USB-stick ooit nog automatisch bedreigingen uitvoert. Zodra een USB-apparaat immuun is gemaakt, kunnen bedreigingen het niet langer configureren om een bepaalde toepassing uit te voeren wanneer het apparaat wordt verbonden met een Windows-apparaat.

Om een USB-apparaat te immuniseren:

1. Verbind de USB-stick met uw apparaat.
2. Blader op uw apparaat naar de locatie van het verwijderbare opslagapparaat en rechterklik op het pictogram ervan.
3. Ga in het contextuele menu naar **Bitdefender** en selecteer **Deze schijf immuniseren**.

> **Opmerking**
> Als het station al immuun is gemaakt, verschijnt het bericht **Het USB-apparaat wordt beveiligd tegen op autorun gebaseerde bedreigingen** in plaats van de optie Immuniseren.

Om te voorkomen dat uw apparaat bedreigingen start vanaf USB-apparaten die niet immuun zijn gemaakt, kunt u de media autorun-functie uitschakelen. Zie "*De automatische kwetsbaarheidsbewaking gebruiken*" (p. 103) voor meer informatie.

HULPPROGRAMMA'S

23. PROFIELEN

Dagelijkse werkactiviteiten, films kijken of games spelen kan het systeem vertragen, met name wanneer ze tegelijkertijd worden uitgevoerd met het Windows-updateproces en onderhoudstaken. Met Bitdefender kunt u nu uw voorkeursprofiel kiezen en toepassen. Het maakt systeemafstellingen om de prestaties van specifieke geïnstalleerde toepassingen te verbeteren.

Bitdefender verschaft de volgende profielen:

- Werkprofiel
- Filmprofiel
- Gameprofiel
- Openbaar Wifi-profiel
- Profiel Accumodus

Als u besluit om **Profielen** niet te gebruiken, wordt er een standaardprofiel ingeschakeld genaamd **Standaard** dat geen optimalisering verschaft aan uw systeem.

Afhankelijk van uw activiteit worden de volgende productinstellingen toegepast als er Werk-, Film- of Gameprofielen geactiveerd zijn:

- Alle Bitdefender waarschuwingen en pop-ups zijn uitgeschakeld.
- Automatische Update wordt uitgesteld.
- Geplande scans zijn uitgesteld.
- Search Advisor is uitgeschakeld.
- Meldingen bijzondere aanbiedingen zijn uitgeschakeld

Afhankelijk van uw activiteit worden de volgende systeeminstellingen toegepast als er Werk-, Film- of Gameprofielen geactiveerd zijn:

- Automatische Windows-updates zijn uitgesteld.
- Windows-waarschuwingen en pop-ups zijn uitgeschakeld.
- Onnodige programma's op de achtergrond worden gestaakt.
- Visuele effecten worden afgesteld voor de beste prestaties.
- Onderhoudstaken worden uitgesteld.

- Instellingen voor het vermogen worden aangepast.

Terwijl u in het Openbare Wi-Fi-profiel werkt, is Bitdefender Antivirus Plus ingesteld om automatisch de volgende programma-instellingen uit te voeren:

- Advanced Threat Defense is ingeschakeld
- De volgende instellingen van Online Threat Prevention zijn ingeschakeld:
  - Versleutelde webscan
  - Bescherming tegen fraude
  - Bescherming tegen phishing

23.1. Werkprofiel

Meerdere taken uitvoeren op het werk, zoals het verzenden van e-mails, een videogesprek hebben met collega's op afstand of werken met designtoepassingen kan invloed hebben op uw systeemprestaties. Werkprofiel is ontworpen om u te helpen uw werkefficiëntie te verbeteren, door een aantal diensten op de achtergrond en onderhoudstaken uit te schakelen.

Werkprofiel configureren

Om de te ondernemen acties te configureren terwijl u in Werkprofiel zit:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Hulpprogramma's**.
2. Klik in het tabblad **Profielen** op **Instellingen**.
3. Klik op de knop **CONFIGUREREN** in het gebied Werkprofiel.
4. Kies de afstellingen voor het systeem die u wilt toepassen door de volgende opties aan te vinken:
   - Prestaties boosten op werktoepassingen
   - Productinstellingen voor Werkprofiel optimaliseren
   - Programma's op de achtergrond en onderhoudstaken uitstellen
   - Automatische Windows-updates uitstellen
5. Klik op **OPSLAAN** om de wijzigingen op te slaan en het venster te sluiten.

Handmatig toepassingen toevoegen aan de lijst Werkprofiel

Indien Bitdefender niet automatisch naar Werkprofiel overschakelt wanneer u een bepaalde werktoepassing opstart, kunt u de toepassing handmatig toevoegen aan de **Werktoepassingenlijst**.

Om toepassingen handmatig toe te voegen aan de Werktoepassingenlijst in Werkprofiel:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Hulpprogramma's**.
2. Klik in het tabblad **Profielen** op **Instellingen**.
3. Klik op de knop **CONFIGUREREN** in het gebied Werkprofiel.
4. In het venster **Instellingen Werkprofiel** klikt u op **Toepassingenlijst**.
5. Klik op **TOEVOEGEN**.

   Er verschijnt een nieuw venster. Blader naar het uitvoerbare bestand van de toepassing, selecteer het en klik op **OK** om het aan de lijst toe te voegen.

23.2. Filmprofiel

Het weergeven van videocontent in HD-kwaliteit, zoals HD-films, vereist belangrijke systeemvermogens. Filmprofiel stelt het systeem- en de productinstellingen af zodat u kunt genieten van een ononderbroken en vloeiende filmervaring.

Filmprofiel configureren

Om de te nemen handelingen te configureren terwijl u in Filmprofiel bent:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Hulpprogramma's**.
2. Klik in het tabblad **Profielen** op **Instellingen**.
3. Klik op de knop **CONFIGUREREN** in het gebied Filmprofiel.
4. Kies de afstellingen voor het systeem die u wilt toepassen door de volgende opties aan te vinken:
   - Prestaties voor videospelers boosten
   - Productinstellingen voor Filmprofiel optimaliseren
   - Programma's op de achtergrond en onderhoudstaken uitstellen
   - Automatische Windows-updates uitstellen

- Instellingen vermogensplan voor films afstellen.

5. Klik op **OPSLAAN** om de wijzigingen op te slaan en het venster te sluiten.

Handmatig videospelers toevoegen aan de lijst Filmprofiel

Indien Bitdefender niet automatisch naar Filmprofiel overschakelt wanneer u een bepaalde videospeler start, kunt u de toepassing handmatig toevoegen aan de **Filmtoepassingenlijst**.

Om videospelers handmatig toe te voegen aan de Filmtoepassingenlijst in Filmprofiel:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Hulpprogramma's**.
2. Klik in het tabblad **Profielen** op **Instellingen**.
3. Klik op de knop **CONFIGUREREN** in het gebied Filmprofiel.
4. In het venster **Instellingen Werkprofiel** klikt u op **Spelerslijst**.
5. Klik op **TOEVOEGEN**.

   Er verschijnt een nieuw venster. Blader naar het uitvoerbare bestand van de toepassing, selecteer het en klik op **OK** om het aan de lijst toe te voegen.

23.3. Gameprofiel

Genieten van een ononderbroken game-ervaring heeft alles te maken met het verminderen van systeemolaadtijden en het beperken van vertraging. Door gebruik te maken van gedragsheuristiek tegelijk met een lijst van bekende games, kan Bitdefender automatisch uitgevoerde games detecteren en uw systeemvermogen optimaliseren zodat u kunt genieten van uw gametijd.

Gameprofiel configureren

Om de te ondernemen acties te configureren terwijl u in Gameprofiel zit:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Hulpprogramma's**.
2. Klik in het tabblad **Profielen** op **Instellingen**.
3. Klik op de knop **Configureren** in het gebied Gameprofiel.
4. Kies de afstellingen voor het systeem die u wilt toepassen door de volgende opties aan te vinken:

- Prestaties voor games boosten
- Productinstellingen voor Gameprofiel optimaliseren
- Programma's op de achtergrond en onderhoudstaken uitstellen
- Automatische Windows-updates uitstellen
- Instellingen vermogensplan voor games afstellen.

5. Klik op **OPSLAAN** om de wijzigingen op te slaan en het venster te sluiten.

Handmatig games aan de Spellijst toevoegen

Indien Bitdefender niet automatisch naar het Gameprofiel overschakelt wanneer u een bepaalde game of toepassing start, kunt u de toepassing handmatig toevoegen aan de **Gametoepassingenlijst**.

Om games handmatig aan de Gametoepassingenlijst toe te voegen in het Gameprofiel:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Hulpprogramma's**.
2. Klik in het tabblad **Profielen** op **Instellingen**.
3. Klik op de knop **CONFIGUREREN** in het gebied Gameprofiel.
4. In het venster **Instellingen Gameprofiel** klikt u op **Gamelijst**.
5. Klik op **TOEVOEGEN**.

   Er verschijnt een nieuw venster. Blader naar het uitvoerbare bestand van de game, selecteer het en klik op **OK** om het aan de lijst toe te voegen.

23.4. Openbaar Wifi-profiel

E-mailberichten verzenden, gevoelige logingegevens invoeren of online winkelen terwijl u met onveilige draadloze netwerken verbonden bent, kan uw persoonlijke gegevens in gevaar brengen. Openbaar Wifi-profiel past de productinstellingen aan, zodat u online betalingen kunt uitvoeren en gevoelige informatie kunt gebruiken in een beveiligde omgeving.

Openbaar Wi-Fi-profiel configureren

Om Bitdefender configureren zodat productinstellingen worden toegepast wanneer u verbonden bent met een onveilig draadloos netwerk:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Hulpprogramma's**.

2. Klik in het tabblad **Profielen** op **Instellingen**.
3. Klik op de knop **CONFIGUREREN** in het gebied Openbaar Wi-Fi-profiel.
4. Laat het vakje **Pas de productinstellingen aan om de bescherming te stimuleren bij verbinding met een onveilig openbaar Wi-Fi-netwerk** aangevinkt.
5. Klik op **Opslaan**.

23.5. Profiel Accumodus

Het profiel Accumodus is speciaal ontworpen voor laptop- en tabletgebruikers. Het doel ervan is om de invloed op vermogensverbruik van zowel systeem als Bitdefender te beperken als het accuniveau lager is dan de standaardconsumptie van deze die u selecteert.

Profiel Accumodus aan het configureren

Om het profiel Accumodus te configureren:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Hulpprogramma's**.
2. Klik in het tabblad **Profielen** op **Instellingen**.
3. Klik op de knop **Configureren** in het gebied Profiel Accumodus.
4. Kies de afstellingen voor het systeem die moeten worden toegepast door de volgende opties aan te vinken:
   - Productinstellingen voor Accumodus optimaliseren.
   - Programma's op de achtergrond en onderhoudstaken uitstellen.
   - Automatische Windows-updates uitstellen.
   - Instellingen vermogensplan voor Accumodus afstellen.
   - Externe apparaten en netwerkpoorten uitschakelen.
5. Klik op **OPSLAAN** om de wijzigingen op te slaan en het venster te sluiten.

Tik een geldige waarde in het vakje in of selecteer er een met de pijltjes omhoog en om laag om in te stellen wanneer het systeem moet beginnen werken in Batterijmodus. Standaard is de modus geactiveerd als het accuniveau onder de 30% komt.

De volgende productinstellingen worden toegepast als Bitdefender in het profiel Accumodus handelt:

- Bitdefender Automatische Update is uitgesteld.
- Geplande scans zijn uitgesteld.

Bitdefender detecteert wanneer uw laptop overschakelt op accuvoeding en afhankelijk van het accuniveau gaat het dan automatisch over op de Accumodus. Op dezelfde manier verlaat Bitdefender automatisch de Accumodus, als de laptop niet langer op de accu werkt.

23.6. Realtime Optimalisering

Bitdefender Real-Time Optimalisering is een plug-in die uw systeemprestaties geruisloos verbetert, op de achtergrond, en garandeert dat u niet wordt onderbroken terwijl u in een profielmodus bent. Afhankelijk van de CPU-belasting bewaakt de plug-in alle processen en richt zich op die processen die een hogere belasting aannemen om ze aan te passen aan uw behoeften.

Om Realtime-optimalisatie in of uit te schakelen:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Hulpprogramma's**.
2. Klik in het tabblad **Profielen** op **Instellingen**.
3. Verrol naar beneden tot u de optie Optimalisatie in reële tijd ziet, en gebruik vervolgens de bijhorende schakelaar om deze in of uit te schakelen.

24. DATA BESCHERMING

24.1. Bestanden definitief verwijderen

Wanneer u een bestand verwijdert, is het niet langer toegankelijk met de normale middelen. Het bestand blijft echter opgeslagen op de harde schijf tot het wordt overschreven wanneer nieuwe bestanden worden gekopieerd.

Bitdefender Bestandsvernietiging helpt om gegevens permanent te verwijderen door ze fysisch te wissen van uw harde schijf.

Volg deze stappen om bestanden of mappen snel permanent verwijderen van uw apparaat via het contextmenu van Windows:

1. Klik met de rechtermuisknop op het bestand of de map die u permanent wilt verwijderen.
2. Selecteer **Bitdefender** > **Bestandsvernietiging** in het contextmenu dat verschijnt.
3. Klik op **PERMANENT VERWIJDEREN** en bevestig dat u het proces wilt voortzetten.

   Wacht tot Bitdefender het vernietigen van de bestanden heeft voltooid.
4. De resultaten worden weergegeven. Klik op **BEËINDIGEN** om de wizard te verlaten.

U kunt bestanden ook vernietigen via de Bitdefender-interface, als volgt:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Hulpprogramma's**.
2. In het panel **GEGEVENSBEVEILIGING** klikt u op **Bestandsvernietiging**.
3. Volg de wizard Bestandsvernietiging:
   a. Klik op de knop **MAPPEN TOEVOEGEN** om de bestanden of mappen die u permanent wenst te verwijderen, toe te voegen.

      U kunt deze bestanden of mappen ook naar dit venster slepen.
   b. Klik op **PERMANENT VERWIJDEREN** en bevestig dat u het proces wilt voortzetten.

      Wacht tot Bitdefender het vernietigen van de bestanden heeft voltooid.
   c. **Samenvatting resultaten**

De resultaten worden weergegeven. Klik op **BEËINDIGEN** om de wizard te verlaten.

PROBLEMEN OPLOSSEN

25. ALGEMENE PROBLEMEN OPLOSSEN

Dit hoofdstuk beschrijft enkele problemen die zich kunnen voordoen terwijl u Bitdefender gebruikt en biedt u mogelijke oplossingen voor deze problemen. De meeste problemen kunnen worden opgelost door de juiste configuratie van de productinstellingen.

- "*Mijn systeem lijkt traag*" (p. 144)
- "*Het scannen start niet*" (p. 145)
- "*Ik kan een bepaalde toepassing niet meer gebruiken*" (p. 148)
- "*Wat moet u doen wanneer Bitdefender een website, domein, IP-adres of online toepassing blokkeert die veilig is*" (p. 149)
- "*Bitdefender updaten bij een langzame internetverbinding*" (p. 150)
- "*De Bitdefender-services reageren niet*" (p. 150)
- "*De Autofill-functie in mijn Portefeuille werkt niet*" (p. 151)
- "*Het verwijderen van Bitdefender is mislukt*" (p. 152)
- "*Mijn systeem start niet op na het installeren van Bitdefender*" (p. 153)

Als u het probleem hier niet kunt vinden of als de voorgestelde oplossingen niet werken, kunt u contact opnemen met vertegenwoordigers van de technische ondersteuning van Bitdefender zoals beschreven in hoofdstuk "*Hulp vragen*" (p. 165).

25.1. Mijn systeem lijkt traag

Na het installeren van beveiligingssoftware kan er doorgaans een lichte vertraging van het systeem merkbaar zijn. Dit is normaal tot in zekere mate.

Als u een aanzienlijke vertraging opmerkt, kan dit probleem verschijnen door de volgende redenen:

- **Bitdefender is niet het enige beveiligingsprogramma dat op uw systeem is geïnstalleerd.**

  Hoewel Bitdefender de beveiligingsprogramma's verwijdert die tijdens de installatie zijn gevonden, is het aanbevolen elke andere beveiligingsoplossing die u mogelijk gebruikt voordat u Bitdefender installeert, te verwijderen. Zie "*Andere beveiligingsoplossingen verwijderen*" (p. 70) voor meer informatie.

- **Er is niet voldaan aan de systeemvereisten voor het uitvoeren van Bitdefender.**

  Als uw apparaat niet voldoet aan de systeemvereisten wordt de computer trager, vooral wanneer er meerdere toepassingen tegelijk actief zijn. Zie "*Systeemvereisten*" (p. 3) voor meer informatie.

- **U hebt toepassingen geïnstalleerd die u niet gebruikt**.

  Elk apparaat heeft programma's of toepassingen die niet worden gebruikt. En veel ongewenste programma's worden op de achtergrond uitgevoerd en nemen schijfruimte en geheugen in. De-installeer een programma als u het niet gebruikt. Dit geldt ook voor andere vooraf geïnstalleerde software of evaluatietoepassingen die u hebt vergeten te verwijderen.

  > **Belangrijk**
  > Indien u vermoedt dat een programma of toepassing een essentieel deel van uw besturingssysteem uitmaakt, verwijder het dan niet en neem contact op met Bitdefender-klantenservice voor hulp.

- **Uw systeem is mogelijk geïnfecteerd**.

  De snelheid en het algemene gedrag van uw systeem kan ook worden beïnvloed door bedreigingen. Spyware, malware, Trojaanse paarden en adware eisen allemaal hun tol op de prestaties van uw apparaat. Zorg dat u uw systeem periodiek scant, maar minstens eenmaal per week. Het wordt aanbevolen om Bitdefender Systeemscan te gebruiken want deze scant op alle types bedreigingen die de veiligheid van uw systeem in gevaar brengen.

  De Systeemscan starten:

  1. Klik in het navigatiemenu in de Bitdefender-interface op **Bescherming**.
  2. In het deelvenster **ANTIVIRUS** klikt u op **Openen**.
  3. In het venster **Scans** klikt u naast **Systeemscan** op **Scan uitvoeren**.
  4. Volg de stappen van de wizard.

25.2. Het scannen start niet

Dit probleemtype kan twee hoofdoorzaken hebben:

- **Een eerder installatie van Bitdefender die niet volledig werd verwijderd of een ongeldige Bitdefender-installatie**.

Installeer Bitdefender in dat geval opnieuw:

- In **Windows 7**:
  1. Klik op **Start**, ga naar **Configuratiescherm** en dubbelklik op **Programma's en onderdelen**.
  2. **Bitdefender Antivirus Plus** vinden en **De-installeren** selecteren.
  3. Klik op **OPNIEUW INSTALLEREN** in het venster dat verschijnt.
  4. Wacht tot het herinstalleren is voltooid en start vervolgens uw systeem opnieuw op.
- In **Windows 8 en Windows 8.1**:
  1. Zoek vanuit het Windows-startscherm het **Configuratiescherm** (u kunt bijvoorbeeld starten met het typen van "configuratiescherm", rechtstreeks in het startscherm) en klik op het pictogram ervan.
  2. Klik op **Een programma verwijderen** of **Programma's en onderdelen**.
  3. **Bitdefender Antivirus Plus** vinden en **De-installeren** selecteren.
  4. Klik op **OPNIEUW INSTALLEREN** in het venster dat verschijnt.
  5. Wacht tot het herinstalleren is voltooid en start vervolgens uw systeem opnieuw op.
- In **Windows 10**:
  1. Klik op **Start**, klik dan op Instellingen.
  2. Klik op het pictogram **Systeem** in Instellingen, selecteer dan **Geïnstalleerde apps**.
  3. **Bitdefender Antivirus Plus** vinden en **De-installeren** selecteren.
  4. Klik nogmaals op **De-installeren** om uw keuze te bevestigen.
  5. Klik op **OPNIEUW INSTALLEREN** in het venster dat verschijnt.
  6. Wacht tot het herinstalleren is voltooid en start vervolgens uw systeem opnieuw op.

Opmerking

Als u deze procedure voor opnieuw installeren volgt, worden persoonlijke instellingen opgeslagen, die in het nieuw geïnstalleerde product ook beschikbaar blijven. Andere instellingen kunnen teruggesteld worden naar hun fabriekskonfiguratie.

- **Bitdefender is niet de enige beveiligingsoplossing die op uw systeem is geïnstalleerd**.

  In dit geval:

  1. Verwijder de andere beveiligingsoplossing. Zie *"Andere beveiligingsoplossingen verwijderen"* (p. 70) voor meer informatie.
  2. Bitdefender opnieuw installeren
     - In **Windows 7**:
       a. Klik op **Start**, ga naar **Configuratiescherm** en dubbelklik op **Programma's en onderdelen**.
       b. **Bitdefender Antivirus Plus** vinden en **De-installeren** selecteren.
       c. Klik op **OPNIEUW INSTALLEREN** in het venster dat verschijnt.
       d. Wacht tot het herinstalleren is voltooid en start vervolgens uw systeem opnieuw op.
     - In **Windows 8 en Windows 8.1**:
       a. Zoek vanuit het Windows-startscherm het **Configuratiescherm** (u kunt bijvoorbeeld starten met het typen van "configuratiescherm", rechtstreeks in het startscherm) en klik op het pictogram ervan.
       b. Klik op **Een programma verwijderen** of **Programma's en onderdelen**.
       c. **Bitdefender Antivirus Plus** vinden en **De-installeren** selecteren.
       d. Klik op **OPNIEUW INSTALLEREN** in het venster dat verschijnt.
       e. Wacht tot het herinstalleren is voltooid en start vervolgens uw systeem opnieuw op.
     - In **Windows 10**:
       a. Klik op **Start**, klik dan op Instellingen.
       b. Klik op het pictogram **Systeem** in Instellingen, selecteer dan **Geïnstalleerde apps**.
       c. **Bitdefender Antivirus Plus** vinden en **De-installeren** selecteren.
       d. Klik nogmaals op **De-installeren** om uw keuze te bevestigen.
       e. Klik op **OPNIEUW INSTALLEREN** in het venster dat verschijnt.
       f. Wacht tot het herinstalleren is voltooid en start vervolgens uw systeem opnieuw op.

Opmerking
Als u deze procedure voor opnieuw installeren volgt, worden persoonlijke instellingen opgeslagen, die in het nieuw geïnstalleerde product ook beschikbaar blijven. Andere instellingen kunnen teruggesteld worden naar hun fabriekskonfiguratie.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning, zoals beschreven in de sectie "*Hulp vragen*" (p. 165).

25.3. Ik kan een bepaalde toepassing niet meer gebruiken

Dit probleem doet zich voor wanneer u probeert een programma te gebruiken dat normaal werkte vóór de installatie van Bitdefender.

Na installatie van Bitdefender kunt u een van deze situaties tegenkomen:

- U kunt van Bitdefender een bericht ontvangen met de melding dat het programma probeert een wijziging aan te brengen aan het systeem.
- U kunt een foutbericht ontvangen van het programma dat u probeert te gebruiken.

Dit type situatie doet zich voor wanneer Advanced Threat Defense per vergissing toepassingen als schadelijk beschouwt.

Advanced Threat Defense is een Bitdefender-functie die constant toezicht houdt op de toepassingen die op uw systeem draaien en verslag uitbrengt over deze die potentieel schadelijk gedrag vertonen. Omdat deze functie op een heuristisch systeem is gebaseerd, kunnen er gevallen zijn waarbij rechtmatige toepassingen worden gerapporteerd door Advanced Threat Defense.

Wanneer deze situatie zich voordoet, kunt u de respectievelijke toepassing uitsluiten, zodat deze niet wordt gemonitord door Advanced Threat Defense.

Om het programma toe te voegen aan de lijst met uitsluitingen:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Bescherming**.
2. Klik op **Instellingen** in het venster **ADVANCED THREAT DEFENSE**.
3. Klik in het venster **Instellingen** op **Uitzonderingen beheren**.
4. Klik op **+Een uitzondering toevoegen**.

5. Voer in het overeenkomende veld het pad van het uitvoerbare bestand in dat u wilt uitsluiten van het scannen.

   U kunt ook naar het uitvoerbare bestand navigeren door te klikken op de knop Bladeren aan de rechterkant van de interface. Selecteer het bestand en klik op **OK**.

6. Schakel de schakelaar naast **Advanced Threat Defense** in.

7. Klik op **Opslaan**.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning, zoals beschreven in de sectie "*Hulp vragen*" (p. 165).

25.4. Wat moet u doen wanneer Bitdefender een website, domein, IP-adres of online toepassing blokkeert die veilig is

Bitdefender biedt een veilige websurfervaring door al het webverkeer te filteren en alle kwaadaardige content te blokkeren. Het is echter mogelijk dat Bitdefender een website, domein, IP-adres of online toepassing die veilig is, als onveilig beschouwt, waardoor het scannen van HTTP-verkeer door Bitdefender deze onterecht gaat blokkeren.

Als dezelfde pagina of online toepassing of hetzelfde domein of IP-adres herhaaldelijk wordt geblokkeerd, kunt u deze toevoegen aan de uitzonderingen zodat ze niet worden gescand door de engines van Bitdefender, wat een vlottere surfervaring garandeert.

Om een website toe te voegen aan **Uitzonderingen**:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Bescherming**.
2. Klik in het venster **ONLINE THREAT PREVENTION** op **Instellingen**.
3. Klik op **Uitzonderingen beheren**.
4. Klik op **+Een uitzondering toevoegen**.
5. Voer in het overeenkomende veld de naam van de website of van het domein of het IP-adres in dat u wilt toevoegen aan de uitzonderingen.
6. Klik op de schakelaar naast **Online Threat Prevention**.
7. Klik op **Opslaan** om de wijzigingen op te slaan en het venster te sluiten.

U dient enkel websites, domeinen, IP-adressen en toepassingen die u volledig vertrouwt, toe te voegen aan deze lijst. Ze worden uitgesloten van het scannen door de volgende engines: bedreiging, phishing en fraude.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning, zoals beschreven in de sectie "*Hulp vragen*" (p. 165).

25.5. Bitdefender updaten bij een langzame internetverbinding

Als u een langzame internetverbinding hebt (zoals een inbelverbinding), kunnen er fouten optreden tijdens het updaten.

Om uw systeem up to date houden met de nieuwste Bitdefender-informatie-database voor bedreigingen:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Instellingen**.
2. Klik op het tabblad **Update**.
3. Schakel de schakelaar **Stille update** uit.
4. Wanneer een volgende update beschikbaar is, zal u worden gevraagd welke update u wilt downloaden. Selecteer enkel **Handtekeningenupdate**.
5. Bitdefender downloadt en installeert enkel de informatie-database voor bedreigingen.

25.6. De Bitdefender-services reageren niet

Dit artikel helpt u bij het oplossen van de foutmelding **Bitdefender-services reageren niet**. U kunt deze fout aantreffen als volgt:

- Het Bitdefender-pictogram in het systeemvak wordt grijs weergegeven en u krijgt een melding dat de Bitdefender-services niet reageren.
- Het Bitdefender-venster geeft aan dat de Bitdefender-services niet reageren.

De fout kan worden veroorzaakt door een van de volgende omstandigheden:

- tijdelijke communicatiefouten tussen de Bitdefender-services.
- sommige Bitdefender-services zijn gestopt.
- andere beveiligingsoplossingen worden op hetzelfde ogenblik als Bitdefender uitgevoerd.

Probeer de volgende oplossingen om deze fouten op te lossen:

1. Wacht enkele ogenblikken en kijk of er iets verandert. De fout kan tijdelijk zijn.
2. Start de apparaat opnieuw op en wacht enkele ogenblikken tot Bitdefender is geladen. Open Bitdefender om te zien of de fout blijft bestaan. Het probleem wordt doorgaans opgelost door de apparaat opnieuw op te starten.
3. Controleer of er een andere beveiligingsoplossing is geïnstalleerd. Dit kan de normale werking van Bitdefender verstoren. Als dat het geval is, raden wij u aan alle andere beveiligingsoplossingen te verwijderen en vervolgens Bitdefender opnieuw te installeren.

   Zie *"Andere beveiligingsoplossingen verwijderen"* (p. 70) voor meer informatie.

Als de fout zich blijft voordoen, moet u contact opnemen met onze experts voor hulp, zoals beschreven in deel *"Hulp vragen"* (p. 165).

25.7. De Autofill-functie in mijn Portefeuille werkt niet

U hebt uw online gegevens opgeslagen in uw Bitdefender-Wachtwoordmanager en u hebt opgemerkt dat autofill niet werkt. Meestal doet dit probleem zich voor wanneer de Bitdefender-Portefeuille-extensie niet is geïnstalleerd in uw browser.

Om deze situatie op te lossen, volgt u deze stappen:

- In **Internet Explorer:**
  1. Open Internet Explorer.
  2. Klik op Extra.
  3. Klik op Invoegtoepassingen beheren.
  4. Klik op Werkbalken en Uitbreidingen.
  5. Ga naar **Bitdefender-Portefeuille** en klik op **Inschakelen**.
- In **Mozilla Firefox:**
  1. Open Mozilla Firefox.
  2. Klik in de rechterbovenhoek van het scherm op de knop **Menu openen**.
  3. Klik op Add-ons.
  4. Klik op Uitbreidingen.

5. Wijs met de muis op **Bitdefender Portefeuille** en klik op de schakelaar ernaast.

- In **Google Chrome:**

1. Open Google Chrome.
2. Ga naar het Menu-pictogram.
3. Klik op Extra.
4. Klik op Uitbreidingen.
5. Wijs met de muis op **Bitdefender Portefeuille** en klik op de bijhorende schakelaar.

Opmerking
De add-on zal worden ingeschakeld nadat u uw webbrowser opnieuw hebt opgestart.

Controleer nu of de autofill-functie in Portefeuille werkt voor uw online accounts.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning, zoals beschreven in de sectie "*Hulp vragen*" (p. 165).

25.8. Het verwijderen van Bitdefender is mislukt

Indien u uw Bitdefender-product wilt verwijderen en u merkt dat het proces blijft hangen of het systeem bevriest, klik dan op **Annuleren** om de handeling af te breken. Start het systeem opnieuw op als dit niet werkt.

Als het verwijderen mislukt, kunnen er enkele registersleutels en bestanden van Bitdefender achterblijven op uw systeem. Dergelijke herinneringen kunnen een nieuwe installatie van Bitdefender verhinderen. Ze kunnen ook de prestaties en stabiliteit van het systeem beïnvloeden.

Om Bitdefender helemaal van uw systeem te verwijderen:

- In **Windows 7**:

1. Klik op **Start**, ga naar **Configuratiescherm** en dubbelklik op **Programma's en onderdelen**.
2. **Bitdefender Antivirus Plus** vinden en **De-installeren** selecteren.
3. Klik op **VERWIJDEREN** in het venster dat verschijnt.

4. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.

- In **Windows 8 en Windows 8.1**:

  1. Zoek vanuit het Windows-startscherm het **Configuratiescherm** (u kunt bijvoorbeeld starten met het typen van "configuratiescherm", rechtstreeks in het startscherm) en klik op het pictogram ervan.
  2. Klik op **Een programma verwijderen** of **Programma's en onderdelen**.
  3. **Bitdefender Antivirus Plus** vinden en **De-installeren** selecteren.
  4. Klik op **VERWIJDEREN** in het venster dat verschijnt.
  5. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.

- In **Windows 10**:

  1. Klik op **Start**, klik dan op Instellingen.
  2. Klik op het pictogram **Systeem** in Instellingen, selecteer dan **Geïnstalleerde apps**.
  3. **Bitdefender Antivirus Plus** vinden en **De-installeren** selecteren.
  4. Klik nogmaals op **De-installeren** om uw keuze te bevestigen.
  5. Klik op **VERWIJDEREN** in het venster dat verschijnt.
  6. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.

25.9. Mijn systeem start niet op na het installeren van Bitdefender

Als u Bitdefender net hebt geïnstalleerd en het systeem niet langer opnieuw kunt opstarten in de normale modus, kunnen er verschillende redenen zijn voor dit probleem.

Dit wordt zee waarschijnlijk veroorzaakt door een eerdere installatie van Bitdefender die niet goed werd verwijderd of door een andere beveiligingsoplossing die nog steeds op het systeem aanwezig is.

U kunt elke situatie op de volgende manier aanpakken:

- **U had eerder een versie van Bitdefender en hebt deze niet correct verwijderd.**

Om dit probleem op te lossen:

1. Start uw systeem opnieuw op en ga naar de Veilige modus. Om te weten hoe u dit kunt doen, ga naar "*Opnieuw opstarten in Veilige modus*" (p. 71).
2. Bitdefender verwijderen van uw systeem:
   - In **Windows 7**:
     a. Klik op **Start**, ga naar **Configuratiescherm** en dubbelklik op **Programma's en onderdelen**.
     b. **Bitdefender Antivirus Plus** vinden en **De-installeren** selecteren.
     c. Klik op **VERWIJDEREN** in het venster dat verschijnt.
     d. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.
     e. Start uw systeem opnieuw op in normale modus.
   - In **Windows 8 en Windows 8.1**:
     a. Zoek vanuit het Windows-startscherm het **Configuratiescherm** (u kunt bijvoorbeeld starten met het typen van "configuratiescherm", rechtstreeks in het startscherm) en klik op het pictogram ervan.
     b. Klik op **Een programma verwijderen** of **Programma's en onderdelen**.
     c. **Bitdefender Antivirus Plus** vinden en **De-installeren** selecteren.
     d. Klik op **VERWIJDEREN** in het venster dat verschijnt.
     e. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.
     f. Start uw systeem opnieuw op in normale modus.
   - In **Windows 10**:
     a. Klik op **Start**, klik dan op Instellingen.
     b. Klik op het pictogram **Systeem** in Instellingen, selecteer dan **Geïnstalleerde apps**.
     c. **Bitdefender Antivirus Plus** vinden en **De-installeren** selecteren.
     d. Klik nogmaals op **De-installeren** om uw keuze te bevestigen.
     e. Klik op **VERWIJDEREN** in het venster dat verschijnt.

f. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.

g. Start uw systeem opnieuw op in normale modus.

3. Uw Bitdefender reïnstalleren.

- **U had eerder een andere beveiligingsoplossing en u hebt deze niet correct verwijderd.**

  Om dit probleem op te lossen:

  1. Start uw systeem opnieuw op en ga naar de Veilige modus. Om te weten hoe u dit kunt doen, ga naar "*Opnieuw opstarten in Veilige modus*" (p. 71).
  2. Verwijder de andere beveiligingsoplossing van uw systeem:
     - In **Windows 7**:
       a. Klik op **Start**, ga naar **Configuratiescherm** en dubbelklik op **Programma's en onderdelen**.
       b. Zoek de naam van het programma dat u wilt verwijderen en selecteer **Verwijderen**.
       c. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.
     - In **Windows 8 en Windows 8.1**:
       a. Zoek vanuit het Windows-startscherm het **Configuratiescherm** (u kunt bijvoorbeeld starten met het typen van "configuratiescherm", rechtstreeks in het startscherm) en klik op het pictogram ervan.
       b. Klik op **Een programma verwijderen** of **Programma's en onderdelen**.
       c. Zoek de naam van het programma dat u wilt verwijderen en selecteer **Verwijderen**.
       d. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.
     - In **Windows 10**:
       a. Klik op **Start**, klik dan op Instellingen.
       b. Klik op het pictogram **Systeem** in Instellingen, selecteer dan **Geïnstalleerde apps**.

c. Zoek de naam van het programma dat u wilt verwijderen en selecteer **Verwijderen**.

d. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.

Om andere software correct te verwijderen, gaat u naar de betreffende website en voert u het hulpprogramma voor het verwijderen uit of neemt u contact op met ons voor de richtlijnen voor het verwijderen.

3. Start uw systeem opnieuw op in de normale modus en installeer Bitdefender opnieuw.

U hebt de bovenstaande stappen al gevolgd en de situatie is niet opgelost.

Om dit probleem op te lossen:

1. Start uw systeem opnieuw op en ga naar de Veilige modus. Om te weten hoe u dit kunt doen, ga naar "*Opnieuw opstarten in Veilige modus*" (p. 71).
2. Gebruik de optie Systeemherstel van Windows om de apparaat te herstellen naar een eerdere datum voordat u het product Bitdefender installeert.
3. Start het systeem opnieuw op in de normale modus en neem contact op met onze experts voor hulp, zoals beschreven in deel "*Hulp vragen*" (p. 165).

26. BEDREIGINGEN VAN UW SYSTEEM VERWIJDEREN

Bedreigingen kunnen uw systeem op heel wat verschillende manieren beïnvloeden en de benadering van Bitdefender is afhankelijk van het type bedreiging. Omdat bedreigingen vaak hun gedrag veranderen, is het moeilijk een patroon vast te stellen voor hun gedrag en hun acties.

Er zijn situaties wanneer Bitdefender de bedreigingsinfectie niet automatisch kan verwijderen van uw systeem. In dergelijke gevallen is uw tussenkomst vereist.

- "*Noodomgeving*" (p. 157)
- "*Wat moet u doen wanneer Bitdefender dreigingen vindt op uw apparaat?*" (p. 158)
- "*Een bedreiging in een archief opruimen*" (p. 160)
- "*Een bedreiging in een e-mailarchief opruimen*" (p. 161)
- "*Wat moet ik doen als ik vermoed dat een bestand gevaarlijk is?*" (p. 162)
- "*Wat zijn de wachtwoordbeveiligde bestanden in het scanlogboek?*" (p. 162)
- "*Wat zijn de overgeslagen items in het scanlogboek?*" (p. 163)
- "*Wat zijn de overgecomprimeerde bestanden in het scanlogboek?*" (p. 163)
- "*Waarom heeft Bitdefender een geïnfecteerd bestand automatisch verwijderd?*" (p. 163)

Als u het probleem hier niet kunt vinden of als de voorgestelde oplossingen niet werken, kunt u contact opnemen met vertegenwoordigers van de technische ondersteuning van Bitdefender zoals beschreven in hoofdstuk "*Hulp vragen*" (p. 165).

26.1. Noodomgeving

Helpmodus is een Bitdefender-functie waarmee u alle bestaande harde schijfpartities binnen en buiten uw besturingssysteem kunt scannen en desinfecteren.

Bitdefender Noodomgeving is geïntegreerd met Windows RE,

Uw systeem starten in de Helpmodus

U kunt enkel op de volgende manier van uw Bitdefender-product naar de Rescue Environment gaan:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Bescherming**.
2. In het deelvenster **ANTIVIRUS** klikt u op **Openen**.
3. Klik op **Openen** naast **Noodomgeving**.
4. Klik op **Herstarten** in het venster dat verschijnt.

   Bitdefender-Rescue Environment wordt binnen enkele ogenblikken geladen.

Uw systeem scannen in de Noodomgeving

Om uw systeem te scannen in de Noodomgeving:

1. Ga naar de Rescue Environment, zoals beschreven in “Uw systeem starten in de Helpmodus” (p. 158).
2. Het Bitdefender-scanproces start automatisch zodra het systeem is geladen in Rescue Environment.
3. Wacht tot de scan is voltooid. Volg de instructies om een gedetecteerde bedreiging te verwijderen.
4. Om Rescue Environment te verlaten, klikt u op de knop **SLUITEN** in het venster met de scanresultaten.

26.2. Wat moet u doen wanneer Bitdefender dreigingen vindt op uw apparaat?

U ontdekt op een van de volgende manieren dat er een dreiging aanwezig is op uw apparaat:

- U hebt uw apparaat gescand en Bitdefender heeft geïnfecteerde items gevonden.
- Een bedreigingswaarschuwing laat u weten dat Bitdefender een of meerdere bedreigingen op uw apparaat heeft geblokkeerd.

Voer in dergelijke gevallen een update uit van Bitdefender om zeker te zijn dat u over de laatste informatiedatabase over bedreigingen beschikt en voer een systeemscan uit om het systeem te analyseren.

Selecteer de gewenste actie (desinfecteren, verwijderen, naar quarantaine verplaatsen) voor de geïnfecteerde items zodra de systeemscan is voltooid.

Waarschuwing
Als u vermoedt dat het bestand deel uitmaakt van het Windows-besturingssysteem of dat het geen geïnfecteerd bestand is, volgt u deze stappen niet en neemt u zo snel mogelijk contact op met de klantendienst van Bitdefender.

Als de geselecteerde actie niet kan worden ondernemen en het scanlogboek een infectie meldt die niet kan worden verwijderd, moet u de bestanden handmatig verwijderen.

De eerste methode kan worden gebruikt in de normale modus:

1. Schakel de real time-antivirusbeveiliging van Bitdefender uit.
   a. Klik in het navigatiemenu in de Bitdefender-interface op **Bescherming**.
   b. In het deelvenster **ANTIVIRUS** klikt u op **Openen**.
   c. Schakel **Bitdefender Shield** uit in het venster **Shield**.
2. Verborgen objecten weergeven in Windows. Om te weten hoe u dit kunt doen, ga naar "*Verborgen objecten weergeven in Windows*" (p. 69).
3. Blader naar de locatie van het geïnfecteerde bestand (controleer het scanlogboek) en verwijder het.
4. Schakel de real time antivirusbeveiliging van Bitdefender in.

Indien de eerste methode niet werkte om de infectie te verwijderen:

1. Start uw systeem opnieuw op en ga naar de Veilige modus. Om te weten hoe u dit kunt doen, ga naar "*Opnieuw opstarten in Veilige modus*" (p. 71).
2. Verborgen objecten weergeven in Windows. Om te weten hoe u dit kunt doen, ga naar "*Verborgen objecten weergeven in Windows*" (p. 69).
3. Blader naar de locatie van het geïnfecteerde bestand (controleer het scanlogboek) en verwijder het.
4. Start uw systeem opnieuw op en ga naar de normale modus.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning, zoals beschreven in de sectie "*Hulp vragen*" (p. 165).

26.3. Een bedreiging in een archief opruimen

Een archief is een bestand of een verzameling van bestanden dat is gecomprimeerd onder een speciale indeling om de benodigde schijfruimte voor het opslaan van de bestanden te beperken.

Sommige van deze formaten zijn open formaten. Hierdoor kan Bitdefender binnen deze formaten scannen en de geschikte acties ondernemen om ze te verwijderen.

Andere archiefformaten worden gedeeltelijk of volledig gesloten. Bitdefender kan alleen de aanwezigheid van bedreigingen detecteren, maar kan geen andere acties ondernemen.

Als Bitdefender u meldt dat er een bedreiging is gedetecteerd binnen een archief en er geen actie beschikbaar is, betekent dit dat het niet mogelijk is de bedreiging te verwijderen vanwege beperkingen op de machtigingsinstellingen voor het archief.

Een bedreiging die in een archief is opgeslagen, wordt op de volgende manier opgeruimd:

1. Identificeer het archief dat de bedreiging bevat door een systeemscan uit te voeren.
2. Schakel de real time-antivirusbeveiliging van Bitdefender uit.
   a. Klik in het navigatiemenu in de Bitdefender-interface op **Bescherming**.
   b. In het deelvenster **ANTIVIRUS** klikt u op **Openen**.
   c. Schakel **Bitdefender Shield** uit in het venster **Shield**.
3. Ga naar de locatie van het archief en decomprimeer het met een archiveringstoepassing, zoals WinZip.
4. Identificeer het geïnfecteerde bestand en verwijder het.
5. Verwijder het originele archief zodat u zeker bent dat de infectie volledig is verwijderd.
6. Comprimeer de bestanden in een nieuw archief met een archiveringstoepassing zoals WinZip.
7. Schakel de realtime antivirusbescherming van Bitdefender in en voer een Systeemscan uit om zeker te zijn dat er geen andere infecties op het systeem aanwezig zijn.

Opmerking
Het is belangrijk dat u weet dat een bedreiging die is opgeslagen in een archief, geen onmiddellijke bedreiging is voor uw systeem, omdat de bedreiging moet worden gedecomprimeerd en uitgevoerd om uw systeem te kunnen infecteren.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning, zoals beschreven in de sectie "*Hulp vragen*" (p. 165).

26.4. Een bedreiging in een e-mailarchief opruimen

Bitdefender kan ook bedreigingen identificeren in de e-maildatabases en e-mailarchieven die op de schijf zijn opgeslagen.

Het is soms nodig het geïnfecteerde bestand te identificeren met de informatie die is opgegeven in het scanrapport en het handmatig te verwijderen.

Een bedreiging die in een e-mailarchief is opgeslagen, wordt op de volgende manier opgeruimd:

1. Scan de e-maildatabase met Bitdefender.
2. Schakel de real time-antivirusbeveiliging van Bitdefender uit.
   a. Klik in het navigatiemenu in de Bitdefender-interface op **Bescherming**.
   b. In het deelvenster **ANTIVIRUS** klikt u op **Openen**.
   c. Schakel **Bitdefender Shield** uit in het venster **Shield**.
3. Open het scanrapport en gebruik de identificatiegegevens (Onderwerp, Van, Aan) van de geïnfecteerde berichten om ze te zoeken in de e-mailclient.
4. De geïnfecteerde bestanden verwijderen. De meeste e-mailclients verplaatsen het verwijderde bericht ook naar een herstelmap van waar het kan worden hersteld. U moet controleren of dit bericht ook uit deze herstelmap is verwijderd.
5. Comprimeer de map die het geïnfecteerde bericht bevat.
   - In Microsoft Outlook 2007: Klik in het menu Bestand op Gegevensbestandsbeheer. Selecteer de bestanden van de persoonlijke mappen (.pst) die u wilt comprimeren en klik op Instellingen. Klik nu op Compact.

- In Microsoft Outlook 2010 / 2013/ 2016: In het Bestandsmenu klikt u op Info en dan op Accountinstellingen (Accounts toevoegen en verwijderen of bestaande login-instellingen wijzigen). Klik dan op Gegevensbestand, selecteer de bestanden van de persoonlijke mappen (.pst) die u wilt comprimeren en klik op Instellingen. Klik nu op Compact.

6. Schakel de real time antivirusbeveiliging van Bitdefender in.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning, zoals beschreven in de sectie "*Hulp vragen*" (p. 165).

26.5. Wat moet ik doen als ik vermoed dat een bestand gevaarlijk is?

U kunt vermoeden dat een bestand in uw systeem gevaarlijk is, ondanks het feit dat uw Bitdefender-product het niet heeft gedetecteerd.

Om ervoor te zorgen dat uw systeem beschermd is:

1. Voer een **Systeemscan** uit met Bitdefender. Om te weten hoe u dit kunt doen, ga naar "*Hoe kan ik mijn systeem scannen?*" (p. 55).
2. Als het scanresultaat schoon lijkt, maar u nog steeds twijfels hebt en wilt zeker zijn over het bestand, moet u contact opnemen met onze experts zodat wij u kunnen helpen.

   Om te weten hoe u dit kunt doen, ga naar "*Hulp vragen*" (p. 165).

26.6. Wat zijn de wachtwoordbeveiligde bestanden in het scanlogboek?

Dit is slechts een melding die aangeeft dat Bitdefender heeft gedetecteerd dat deze bestanden ofwel door een wachtwoord ofwel door een vorm van codering zijn beveiligd.

De meest gebruikelijke items die door een wachtwoord zijn beveiligd, zijn:

- Bestanden die bij een andere beveiligingsoplossing horen.
- Bestanden die bij het besturingssysteem horen.

Om de inhoud ook daadwerkelijk te scannen, moeten deze bestanden zijn opgehaald of op een andere manier zijn gedecodeerd.

Als deze inhoud zou worden uitgepakt, zou de real time scanner van Bitdefender ze automatisch scannen om uw apparaat beschermd te houden.

Als u die bestanden wilt scannen met Bitdefender, moet u contact opnemen met de productfabrikant voor meer informatie over die bestanden.

Wij raden u aan deze bestanden te negeren omdat ze geen bedreiging vormen voor uw systeem.

26.7. Wat zijn de overgeslagen items in het scanlogboek?

Alle bestanden die in het scanrapport als Overgeslagen worden weergegeven, zijn zuiver.

Voor betere prestaties scant Bitdefender geen bestanden die niet werden gewijzigd sinds de laatste scan.

26.8. Wat zijn de overgecomprimeerde bestanden in het scanlogboek?

Overgecomprimeerde items zijn elementen die niet kunnen worden opgehaald door de scanengine of elementen waarvoor de decoderingstijd te lang zou zijn waardoor het systeem onstabiel zou kunnen worden.

Overgecomprimeerd betekent dat het Bitdefender het scannen binnen dat archief heeft overgeslagen omdat het uitpakken ervan teveel systeemgeheugen zou in beslag nemen. De inhoud zal bij real time toegang worden gescand indien dat nodig is.

26.9. Waarom heeft Bitdefender een geïnfecteerd bestand automatisch verwijderd?

Als er een geïnfecteerd bestand wordt gedetecteerd, zal Bitdefender automatisch proberen dit te desinfecteren. Als de desinfectie mislukt, wordt het bestand naar quarantaine verplaatst om de infectie in te dammen.

Voor specifieke types bedreigingen is desinfectie niet mogelijk omdat het gedetecteerde bestand volledig boosaardig is. In dergelijke gevallen wordt het geïnfecteerde bestand verwijderd van de schijf.

Dit is doorgaans het geval met installatiebestanden die zijn gedownload vanaf onbetrouwbare websites. Als u zelf in een dergelijke situatie terechtkomt, downloadt u het installatiebestand vanaf de website van de fabrikant of een andere vertrouwde website.

CONTACTEER ONS

27. HULP VRAGEN

Bitdefender verschaft haar klanten een ongeëvenaard niveau van snelle en nauwkeurige ondersteuning. Als u problemen ondervindt met of vragen hebt over uw Bitdefender-product, kunt u meerdere online bronnen gebruiken om een oplossing of antwoord te vinden. Tegelijkertijd kunt u ook contact opnemen met de Bitdefender-klantenservice. Onze medewerkers van de klantenservice zullen uw vragen snel beantwoorden en u alle hulp bieden die u nodig hebt.

De "*Algemene problemen oplossen*" (p. 144) sectie biedt de nodige informatie betreffende de vaakst voorkomende problemen tijdens het gebruik van dit product.

Als u geen oplossing voor uw vraag in de geleverde middelen hebt gevonden, kunt u direct contact met ons opnemen:

- "Neem rechtstreeks vanuit Bitdefender Antivirus Plus contact op met ons" (p. 165)
- "Neem contact op met ons via ons online Ondersteuningscentrum" (p. 166)

Neem rechtstreeks vanuit Bitdefender Antivirus Plus contact op met ons

Als u een actieve internetverbinding hebt, kunt u direct vanaf de productinterface contact opnemen met Bitdefender voor hulp.

Volg deze stappen:

1. Klik in het bovenste gedeelte van de Bitdefender-interface op de knop **Ondersteuning**, voorgesteld door een **vraagteken**.
2. U hebt de volgende opties:
   - **GEBRUIKSAANWIJZING**

     Ga naar onze database en zoek de benodigde informatie.
   - **ONDERSTEUNING**

     Raadpleeg onze online artikels en videohandleidingen.
   - **CONTACTEREN**

     Klik op **ONDERSTEUNING CONTACTEREN** om de Support Tool voor Bitdefender op te starten en de Klantendienst te contacteren.

a. Vul het verzendformulier in met de nodige gegevens:
   i. Selecteer het type probleem dat u hebt ondervonden.
   ii. Voer een beschrijving in van het probleem dat zich heeft voorgedaan.
   iii. Klik op **PROBEER DIT PROBLEEM TE REPRODUCEREN** indien u een productprobleem ondervindt. Reproduceer het probleem en klik in het kader HET PROBLEEM REPRODUCEREN op **VOLTOOIEN**.
   iv. Klik op **TICKET BEVESTIGEN**.
b. Vul het formulier verder in met de vereiste gegevens:
   i. Voer uw volledige naam in.
   ii. Voer uw e-mailadres in.
   iii. Duid het selectievakje voor akkoord aan.
   iv. Klik op **DEBUGGINGPAKKET AANMAKEN**.

   Wacht enkele ogenblikken terwijl Bitdefender productgerelateerde informatie verzamelt. Deze informatie zal onze technici helpen een oplossing voor uw probleem te vinden.
c. Klik op **SLUITEN** om de wizard af te sluiten. Een van onze vertegenwoordigers contacteert u zo snel mogelijk.

Neem contact op met ons via ons online Ondersteuningscentrum

Als u de benodigde informatie niet kunt openen met het Bitdefender-product, kunt u ons online ondersteuningscentrum raadplegen:

1. Ga naar https://www.bitdefender.com/support/consumer.html.

   Het Ondersteuningscentrum van Bitdefender bevat talrijke artikelen met oplossingen voor problemen met betrekking tot Bitdefender.
2. Gebruik de zoekbalk bovenaan het venster om artikelen te vinden die een oplossing voor uw probleem bieden. Vul om te zoeken een term in de zoekbalk in en klik op **Zoeken**.
3. Lees de relevante artikelen of documenten door en pas de voorgestelde oplossingen toe.
4. Als uw probleem hiermee niet is opgelost, gaat u naar

https://www.bitdefender.com/support/contact-us.htmlen neemt u contact op met onze experts van de ondersteuning.

27.1. Telefonische ondersteuning:

De laboratoria van Bitdefender stellen alles in het werk om de toegang tot telefonische ondersteuning te kunnen garanderen, tijdens plaatselijke werkuren van maandag tot en met vrijdag, met uitzondering van feestdagen.

Telefonische toegang tot de laboratoria van Bitdefender:

- **Belgium**: +32 28 91 98 90
- **Netherlands**: 020 788 61 50

Zorg voordat u ons belt dat u de volgende zaken binnen handbereik hebt:

- het licentienummer van uw Bitdefender programma. Geef dit nummer door aan een van onze technici zodat hij kan nagaan op welk type ondersteuning u recht hebt.
- de actuele versie van uw besturingssysteem.
- informatie met betrekking tot de merken en modellen van alle op uw computer aangesloten randapparaten en van de software die in het geheugen is geladen of in gebruik is.

In het geval er een bedreigingen is ontdekt, kan de technicus u vragen om een lijst met technische informatie en bepaalde bestanden door te sturen, die mogelijkerwijs nodig zijn voor het stellen van een diagnose.

Indien een technicus u om foutmeldingen vraagt, geef dan de exacte inhoud door en het moment waarop de meldingen verschenen, de activiteiten die eraan voorafgingen en de stappen die u zelf reeds hebt ondernomen om het probleem op te lossen.

De technicus zal een strikte procedure opvolgen in een poging het probleem op te sporen.

De volgende elementen vallen niet binnen de service:

- Deze technische ondersteuning heeft geen betrekking op de toepassingen, installaties, de deïnstallatie, de overdracht, preventief onderhoud, de vorming, het beheer op afstand of andere softwareconfiguraties dan diegene die tijdens de interventie specifiek door onze technicus werden vermeld.

- De installatie, de instellingen, de optimalisering en de netwerkconfiguratie of de configuratie op afstand van toepassingen die niet binnen het kader van de geldende ondersteuning vallen.
- Back-ups van software/gegevens. De klant dient zelf een back-up te maken van alle gegevens, software en bestaande programma's die aanwezig zijn op de informatiesystemen waarop onze ondersteuning van toepassing is, alvorens enige dienstprestatie te laten uitvoeren door Bitdefender.

Bitdefender KUNNEN IN GEEN GEVAL AANSPRAKELIJK WORDEN GESTELD VOOR HET VERLIES OF DE RECUPERATIE VAN GEGEVENS, PROGRAMMA'S, OF VOOR HET NIET KUNNEN BENUTTEN VAN SYSTEMEN OF VAN HET NETWERK.

Adviezen beperken zich enkel tot de gestelde vragen en zijn gebaseerd op de door de klant verschafte informatie. De problemen en mogelijke oplossingen kunnen afhangen van het type systeemomgeving en van een groot aantal andere variabelen waarvan Bitdefender niet op de hoogte zijn.

Bitdefender kunnen dan ook in geen geval aansprakelijk worden gesteld voor eventuele schade die voortvloeit uit het gebruik van de verschafte informatie.

Het kan zijn dat het systeem waarop de Bitdefender programma's moeten worden geïnstalleerd onstabiel is (eerdere virusinfecties, installatie van meerdere antivirus - of beveiligingsprogramma's, etc.). In betreffende gevallen zal een technicus u mogelijkerwijze voorstellen eerst een onderhoudsbeurt op uw systeem te laten uitvoeren, alvorens het probleem kan worden opgelost.

De technische gegevens kunnen wijzigen op het moment dat er nieuwe gegevens beschikbaar zijn. Om die reden raden Bitdefender u dan ook aan regelmatig onze site "Producten" te raadplegen, via https://www.bitdefender.nl voor upgrades, of onze site met veelgestelde vragen (FAQ) op https://www.bitdefender.nl/support/consumer/.

Bitdefender wijzen elke aansprakelijkheid af voor enige rechtstreekse, onrechtstreekse, bijzondere of accidentele schade, of voor gevolgschade die te wijten is aan het gebruik van de aan u verschafte informatie.

Indien een interventie ter plaatse noodzakelijk is, zal de technicus u meer gedetailleerde informatie verschaffen met betrekking tot de dichtstbijzijnde wederverkoper.

28. ONLINE BRONNEN

Er zijn meerdere online informatiebronnen beschikbaar om u te helpen bij het oplossen van problemen en vragen met betrekking tot Bitdefender.

- Ondersteuningscentrum voor Bitdefender:

  https://www.bitdefender.com/support/consumer.html

- Ondersteuningsforum voor Bitdefender:

  https://forum.bitdefender.com

- Het HOTforSecurity-portaal over computerbeveiliging:

  https://www.hotforsecurity.com

U kunt ook uw favoriete zoekmachine gebruiken om meer informatie te zoeken over computerbeveiliging, de Bitdefender-producten en het bedrijf.

28.1. Ondersteuningscentrum voor Bitdefender

Het Bitdefender Ondersteuningscentrum is een online opslagplaats van informatie over Bitdefender-producten. Hier worden rapporten bijgehouden in een gemakkelijk toegankelijk formaat over de doorlopende technische ondersteuning en activiteiten voor foutoplossingen van de ondersteunings- en ontwikkelingsteams van Bitdefender. Daarnaast vindt u hier ook meer algemene artikels over preventie tegen bedreigingen, het beheer van Bitdefender-oplossingen met gedetailleerde uitleg en talrijke andere artikels.

Het Bitdefender Ondersteuningscentrum is toegankelijk voor iedereen en kan vrij worden doorzocht. De uitgebreide informatie in deze database is een van de vele middelen om Bitdefender-klanten toegang te geven tot technische kennis en waardevolle inzichten. Alle geldige aanvragen voor informatie of foutrapporten die van Bitdefender-klanten komen, vinden uiteindelijk hun weg naar het Bitdefender-ondersteuningscentrum, als rapporten over het oplossen van problemen, “spiekbriefjes” om een probleem te omzeilen of informatieve artikels om de helpbestanden van het product aan te vullen.

Het Bitdefender Ondersteuningscentrum is elk uur van de dag beschikbaar op

https://www.bitdefender.com/support/consumer.html.

28.2. Bitdefender Ondersteuningsforum

Het Bitdefender Ondersteuningsforum biedt Bitdefender-gebruikers een eenvoudige manier om hulp te krijgen en anderen te helpen.

Als uw Bitdefender-product niet goed werkt, als bepaalde bedreigingen niet van uw apparaat worden verwijderd of als u iets wilt vragen over de werking van het product, kunt u dit melden of vragen op het forum.

Bitdefender-ondersteuningstechnici controleren het forum en plaatsen nieuwe informatie om u te helpen. U kunt ook een antwoord of oplossing krijgen van een meer ervaren Bitdefender-gebruiker.

Zoek altijd eerst op het forum om te zien of een vergelijkbare vraag of kwestie al eerder is besproken.

Het Bitdefender Ondersteuningsforum is op https://forum.bitdefender.com beschikbaar in 5 verschillende talen: Engels, Duits, Frans, Spaans en Roemeens. Klik op de koppeling **Home & Home Office Protection** om toegang te krijgen tot het gebied voor verbruiksproducten.

28.3. HOTforSecurity-portaal

HOTforSecurity is een rijke bron aan informatie over computerbeveiliging. Hier leert u meer over de verschillende bedreigingen waaraan uw apparaat wordt blootgesteld wanneer u een verbinding met Internet maakt (malware, phishing, spam, cybercriminelen).

Er worden regelmatig nieuwe artikelen gepubliceerd om u op de hoogte te houden van de meest recent ontdekte bedreigingen, actuele beveiligingstrends en andere informatie over de beveiligingssector.

De webpagina van HOTforSecurity is https://www.hotforsecurity.com.

29. CONTACTINFORMATIE

Efficiënte communicatie is de sleutel naar het succes. BITDEFENDER heeft sinds 2001 een onberispelijke reputatie opgebouwd door voortdurend te streven naar een betere communicatie om de verwachtingen van onze klanten en partners te overtreffen. Aarzel niet contact op te nemen met ons als u eventuele vragen hebt.

29.1. Webadressen

Verkoopafdeling: sales@bitdefender.com
Ondersteuningscentrum:https://www.bitdefender.com/support/consumer.html
Documentatie: documentation@bitdefender.com
Lokale distributeurs:https://www.bitdefender.com/partners
Partnerprogramma: partners@bitdefender.com
Persinformatie: pr@bitdefender.com
Vacatures: jobs@bitdefender.com
Indienen van bedreigingen: virus_submission@bitdefender.com
Spammeldingen: spam_submission@bitdefender.com
Misbruikmeldingen: abuse@bitdefender.com
Website:https://www.bitdefender.be

29.2. Lokale verdelers

De lokale Bitdefender-verdelers zijn altijd paraat om te reageren op aanvragen met betrekking tot hun bedrijfsgebied, zowel op commercieel als algemeen vlak.

Een Bitdefender-verdeler in uw land zoeken:

1. Ga naar https://www.bitdefender.com/partners/partner-locator.html.
2. Kies uw land en stad met de overeenkomstige opties.
3. Als u geen Bitdefender-distributeur in uw land kunt vinden, kunt u via email rechtstreeks contact met ons opnemen via sales@bitdefender.com. Schrijf uw e-mail in het Engels zodat wij u onmiddellijk kunnen helpen.

29.3. Bitdefender-kantoren

De Bitdefender-kantoren zijn altijd paraat om te reageren op aanvragen met betrekking tot hun bedrijfsgebied, zowel op commercieel als algemeen vlak.

Hun respectievelijke adressen en contactpersonen worden hieronder weergegeven:

België

Bitdefender SAS
49, Rue de la Vanne
92120 Montrouge
Telefoon: +33 (0)1 47 35 72 73
Verkoop: sales@bitdefender.com
Technische ondersteuning: https://www.bitdefender.be/support/contact-us
Web: https://www.bitdefender.be

Verenigde Staten

Bitdefender, LLC
6301 NW 5th Way, Suite 4300
Fort Lauderdale, Florida 33309
Telefoon (kantoor&verkoop): 1-954-776-6262
Verkoop: sales@bitdefender.com
Technische ondersteuning: https://www.bitdefender.com/support/consumer.html
Web: https://www.bitdefender.com

VK en Ierland

BITDEFENDER LTD
C/O Howsons Winton House, Stoke Road, Stoke on Trent
Staffordshire, United Kindon, ST4 2RW
E-mail: info@bitdefender.co.uk
Telefoon: (+44) 2036 080 456
Verkoop: sales@bitdefender.co.uk
Technische ondersteuning: https://www.bitdefender.co.uk/support/
Web: https://www.bitdefender.co.uk

Duitsland

Bitdefender GmbH
TechnoPark Schwerte
Lohbachstrasse 12
D - 58239 Schwerte

Kantoor: +49 2304 9 45 - 162
Fax: +49 2304 9 45 - 169
Verkoop: vertrieb@bitdefender.de
Technische ondersteuning: https://www.bitdefender.de/support/consumer.html
Web: https://www.bitdefender.de

Denemarken

Bitdefender APS
Agern Alle 24, 2970 Hørsholm, Denmark
Kantoor: +45 7020 2282
Technische ondersteuning: http://bitdefender-antivirus.dk/
Web: http://bitdefender-antivirus.dk/

Spanje

Bitdefender España, S.L.U.
C/Bailén, 7, 3-D
08010 Barcelona
Fax: +34 93 217 91 28
Telefoon: +34 902 19 07 65
Verkoop: comercial@bitdefender.es
Technische ondersteuning: https://www.bitdefender.es/support/consumer.html
Website: https://www.bitdefender.es

Roemenië

BITDEFENDER SRL
Orhideea Towers Building, 15A Orhideelor Street, 11th fllor, district 6
Bucharest
Fax: +40 21 2641799
Telefoon verkoop: +40 21 2063470
E-mail verkoop: sales@bitdefender.ro
Technische ondersteuning: https://www.bitdefender.ro/support/consumer.html
Website: https://www.bitdefender.ro

Verenigde Arabische Emiraten

Dubai Internet City
Building 17, Office # 160
Dubai, UAE
Telefoon verkoop: 00971-4-4588935 / 00971-4-4589186
E-mail verkoop: mena-sales@bitdefender.com
Technische ondersteuning: https://www.bitdefender.com/support/consumer.html
Website: https://www.bitdefender.com

Woordenlijst

Abonnement

Koopovereenkomst die u het recht heeft om een specifiek(e) product of dienst op een specifiek aantal toestellen en voor een bepaalde tijd te gebruiken. Een vervallen abonnement kan automatisch worden verlengd met gebruik van de informatie van de gebruiker tijdens de eerste aankoop.

Achterdeur

Een gat in de beveiliging van een systeem, dat opzettelijk werd achtergelaten door ontwikkelaars of beheerders. De motivatie voor dergelijke gaten is niet altijd boosaardig. Sommige besturingssystemen worden bijvoorbeeld geleverd met bevoegde accounts die bedoeld zijn voor gebruik door technici voor service ter plaatse of onderhoudsprogrammeurs van verkopers.

Activeringscode

Is een unieke sleutel die u in de handel kunt kopen en die gebruikt wordt om een specifiek product of een dienst te activeren. Met een activeringscode kan een geldig abonnement voor een bepaalde periode en een bepaald aantal toestellen geactiveerd worden en kunt u ook gebruiken om het abonnement te verlengen, op voorwaarde dat het voor hetzelfde product of dezelfde dienst is.

ActiveX

ActiveX is een model voor het schrijven van programma's zodat andere programma's en het besturingssysteem ze kunnen oproepen. De ActiveX-technologie wordt gebruikt bij Microsoft Internet Explorer om interactieve Webpagina's te maken die eruitzien en zich gedragen als computerprogramma's in plaats van statische pagina's. Met ActiveX kunnen gebruikers vragen stellen of beantwoorden, drukknoppen gebruiken en op andere manieren interactief omgaan met de Webpagina. ActiveX-besturingselementen zijn vaak geschreven met de hulp van Visual Basic.

ActiveX is berucht door een compleet gebrek aan beveiligingscontroles; computerbeveiligingsexperts raden het gebruik ervan via het internet sterk af.

Adware

Adware wordt vaak gecombineerd met een hosttoepassing die gratis wordt aangeboden op voorwaarde dat de gebruiker akkoord gaat met het uitvoeren van de adware. Omdat adware-toepassingen doorgaans worden geïnstalleerd nadat de gebruiker een licentieovereenkomst die het doel van de toepassing vermeldt heeft geaccepteerd, wordt er geen inbreuk gepleegd.

Pop-upadvertenties kunnen echter irritant worden en in sommige gevallen de systeemprestaties negatief beïnvloeden. De gegevens die door sommige van deze toepassingen worden verzameld, kunnen bovendien privacy-problemen veroorzaken voor gebruikers die niet volledig op de hoogte waren van de voorwaarden van de licentieovereenkomst.

Archief

Een schijf, tape, of map die bestanden bevat waarvan een back-up werd gemaakt.

Een bestand dat één of meer bestanden bevat in een gecomprimeerd formaat.

Bedreiging

Een programma of een deel van een code die op uw computer wordt geladen zonder uw medeweten en tegen uw wil wordt uitgevoerd. De meeste bedreigingen kunnen zichzelf ook dupliceren. Alle computerbedreigingen zijn door de mens gemaakt. Een eenvoudige bedreiging die zichzelf steeds opnieuw kan dupliceren is relatief eenvoudig te maken. Zelfs een dergelijke eenvoudige bedreiging is gevaarlijk aangezien het snel al het beschikbare geheugen zal opgebruiken en het systeem zal blokkeren. Een nog gevaarlijker type is een bedreiging die in staat is zichzelf te verzenden via netwerken en beveiligingssystemen te omzeilen.

Bestandsnaamextensie

Het gedeelte van een bestandsnaam achter de punt, waarmee het gegevenstype dat in het bestand is opgeslagen wordt aangeduid.

Heel wat besturingssystemen, zoals Unix, VMS en MS-DOS, maken gebruik van bestandsextensies. Ze gebruiken doorgaans één tot drie letters (sommige betreurenswaardige oude besturingssystemen ondersteunen niet meer dan drie letters). Voorbeelden hiervan zijn "c" voor C-broncode, "ps" voor PostScript, "txt" voor tekst zonder opmaak.

Botnet

Het woord "botnet" is samengesteld uit de woorden "robot" en "netwerk". Botnets zijn apparaten die met het internet verbonden zijn en met bedreigingen geïnfecteerd zijn en kunnen gebruikt worden om spammail te verzenden, data te stelen, kwetsbare apparaten van op afstand te controleren of om spyware, ransomware en andere schadelijke bedreigingen te verspreiden. Het doel ervan is zoveel mogelijk apparaten te infecteren, bijvoorbeeld pc's, servers, mobiele of IoT-apparaten die eigendom zijn van grote bedrijven of sectoren.

Browser

De korte naam voor Webbrowser, een softwaretoepassing die wordt gebruikt op Webpagina's te zoeken en weer te geven. Populaire browsers omvatten Microsoft Internet Explorer, Mozilla Firefox en Google Chrome. Dit zijn grafische browsers. Dit betekent dat ze zowel grafische beelden als tekst kunnen weergeven. Bovendien kunnen de meeste moderne browsers ook multimedia-informatie voorstellen met geluid en video, hoewel voor sommige formaten plug-ins vereist zijn.

Brute force-aanval

Aanval via raden van wachtwoord, gebruikt om in te breken in een computersysteem door mogelijke wachtwoordcombinaties in te geven, meestal te beginnen met het meest eenvoudig te raden wachtwoord.

Cookie

Binnen de Internetindustrie worden cookies beschreven als kleine programma's die informatie bevatten over individuele computers, die door adverteerders wordt geanalyseerd en gebruikt om uw on line interesse en smaak te volgen. De cookietechnologie wordt in dit kader nog steeds verder ontwikkeld met het doel reclameberichten rechtstreeks te richten op de interesses die u hebt meegedeeld. Dit is voor veel mensen een mes dat aan twee kanten snijdt. Aan de ene kant is het efficiënt en relevant aangezien u alleen reclames ontvangt voor zaken waarvoor u interesse hebt. Aan de andere kant betekent het ook dat elke plaats die u bezoekt en alles wat u aanklikt wordt "opgespoord" en "gevolgd". Het is dan ook te begrijpen dat er heel wat wordt gedebatteerd over privacy. Bovendien zijn veel mensen verontwaardigd omdat ze het gevoel hebben dat ze als een "SKU-nummer" worden beschouwd (u weet wel, de barcode op de verpakkingen die bij de kassa van het warenhuis wordt gescand).

Hoewel dit standpunt misschien nogal extreem is, is het vaak een bijzonder nauwkeurige omschrijving.

Cyberpesten

Wanneer collega's of onbekenden met opzet onrechtmatige daden stellen tegenover kinderen, met de bedoeling om fysiek te kwetsen. Om emotionele schade te berokkenen, sturen de daders gemene berichten of onflatteuze foto's om hun slachtoffers af te zonderen van anderen of gefrustreerd te doen voelen.

Downloaden

Om gegevens (meestal een volledig bestand) te kopiëren van een hoofdbron naar een randapparaat. De term wordt vaak gebruikt om het proces te beschrijven waarbij een bestand van een on line-service wordt gekopieerd naar de eigen computer. Downloaden kan ook verwijzen naar het kopiëren van een bestand van een netwerkbestandsserver naar een computer in het netwerk.

E-mail

Elektronische post. Een dienst die berichten naar computers verzendt via lokale of globale netwerken.

Exploits

Een manier om misbruik te maken van verschillende bugs of kwetsbaarheden in een computer (software of hardware). Zo kunnen hackers de controle over computers of over netwerken in handen krijgen.

Geavanceerde aanhoudende dreiging

Geavanceerde aanhoudende dreiging (Advanced Persistent Threat - APT) maakt misbruik van kwetsbare plekken in systemen om belangrijke informatie te stelen en aan de bron te leveren. Grote groepen, zoals organisaties, bedrijven of overheden zijn doelgroepen voor deze bedreiging.

Het doel van een advanced persistent threat is heel lang onopgemerkt te blijven en belangrijke informatie in te kijken en te verzamelen, zonder de toestellen te beschadigen. De methode die gebruikt wordt om de bedreiging in het netwerk te brengen verloopt via een pdf-bestand of een Office-document dat er onschuldig uitziet, zoadat elke gebruiker de bestanden kan openen.

Gebeurtenissen

Een actie of gebeurtenis die door een programma wordt gedetecteerd. Gebeurtenissen kunnen gebruikersacties zijn, zoals het klikken met de muis of het indrukken van een toets, of systeemgebeurtenissen, zoals een tekort aan geheugen.

Geheugen

Interne opslaggebieden in de computer. De term geheugen staat voor gegevensopslag die in de vorm van chips wordt geleverd. Het woord opslag wordt gebruikt voor geheugen dat aanwezig is op tapes of schijven. Elke computer wordt geleverd met een bepaalde hoeveelheid fysiek geheugen, dat meestal het hoofdgeheugen of RAM wordt genoemd.

Heuristisch

Een methode voor het identificeren van nieuwe bedreigingen op basis van regels. Deze scanmethode is niet gebaseerd op een specifieke informatie-database voor bedreigingen. Het voordeel van de heuristische scan is dat hij zich niet laat misleiden door een nieuwe variant van een bestaande bedreiging. Dit type kan echter af en toe een verdachte code rapporteren in normale programma's, zodat de zogenoemde "valse positieve" rapporten worden gegenereerd.

Honingpot

Een afleiding in uw computersysteem dat hackers aantrekt om te onderzoeken hoe ze te werk gaan en de afwijkende methodes die ze gebruiken om systeeminformatie te verzamelen, te identificeren. Bedrijven zijn steeds meer geïnteresseerd om honingpotten te implementeren en te gebruiken om hun algemene beveiligingsstatus te verbeteren.

Informatie-update Bedreigingen

Het binaire patroon van een bedreiging, gebruikt door de beveiligingsoplossing om de bedreiging te detecteren en te verwijderen.

Ingepakte programma's

Een bestand in een gecomprimeerd formaat. Talrijke besturingssystemen en toepassingen beschikken over opdrachten waarmee u bestanden kunt inpakken, zodat ze minder geheugen in beslag nemen. Veronderstel bijvoorbeeld dat u een tekstbestand hebt dat tien opeenvolgende spatietekens bevat. Normaal zou dit tien bytes opslagruimte vereisen.

Een programma dat bestanden inpakt zou echter de spatietekens vervangen door een speciaal spatiereeks-teken, gevolgd door het aantal spaties dat wordt vervangen. In dit geval zouden de tien spaties slechts twee bytes nodig hebben. Dit is slechts één inpaktechniek, maar er zijn er veel meer.

IP

Internet Protocol - Een routeerbaar protocol in de TCP/OP-protocolreeks die verantwoordelijk is voor de IP-adressering, routing en de fragmentatie en defragmentatie van IP-pakketten.

Java-applet

Een Java-programma dat is ontwikkeld om alleen op een webpagina te worden uitgevoerd. Om een applet op een webpagina te gebruiken, zou u de naam van het applet opgeven en de grootte (lengte en breedte in pixels) die het applet kan gebruiken. Wanneer de webpagina wordt geopend, downloadt de browser het applet van een server en voert hij het uit op de computer van de gebruiker (de client). Applets onderscheiden zich van toepassingen omdat ze worden beheerd door een streng beveiligingsprotocol.

Zelfs wanneer applets bijvoorbeeld op de client worden uitgevoerd, kunnen ze geen gegevens lezen van of schrijven naar de computer van de client. Bovendien worden applets verder beperkt zodat ze alleen gegevens kunnen lezen van en schrijven naar hetzelfde domein waarvan ze worden bediend.

Keylogger

Een keylogger is een toepassing die alles wat u typt, logt.

Keyloggers zijn in wezen niet kwaadaardig. Ze kunnen worden gebruikt voor rechtmatige doeleinden, zoals het bewaken van de activiteiten van werknemers of kinderen. Ze worden echter steeds meer gebruikt door cybercriminele voor boosaardige doeleinden (bijv. voor het verzamelen van persoonlijke gegevens, zoals aanmeldingsgegevens en nummer van de sociale zekerheid).

Macrovirus

Een type computerbedreiging die is gecodeerd als een macro die in een document is ingesloten. Talrijke toepassingen, zoals Microsoft Word en Excel, ondersteunen krachtige macrotalen.

Met deze toepassingen kan u een macro in een document insluiten, en die macro telkens laten uitvoeren wanneer het document wordt geopend.

Mailclient

Een e-mailclient is een toepassing waarmee u e-mail kunt verzenden en ontvangen.

Niet-heuristisch

Deze scanmethode is gebaseerd op een specifieke informatie-database voor bedreigingen. Het voordeel van de niet-heuristische scan is dat deze zich niet laat misleiden door iets dat kan lijken op een bedreiging en geen vals alarm genereert.

Online kinderlokkers

Personen die minderjarigen of adolescenten met opzet willen betrekken in gesprekken, om hen zo te betrekken in illegale seksuele activiteiten. Sociale netwerken zijn de ideale plaats waar kwetsbare kinderen gemakkelijk kunnen worden verleid om seksuele activiteiten uit te voeren, online of tijdens fysieke ontmoetingen.

Opdrachtregel

In een opdrachtregelinterface typt de gebruiker opdrachten in opdrachttaal rechtstreeks op het scherm in de ruimte die hiervoor wordt geboden.

Opstartitems

Elk bestand in deze map wordt geopend wanneer de computer wordt gestart. Een opstartitem kan bijvoorbeeld een opstartscherm zijn, een geluidsbestand dat moet worden afgespeeld wanneer de computer voor de eerste maal opstart, een herinneringsagenda of apps. In normale omstandigheden wordt een alias van een bestand in deze map geplaatst, en niet het bestand zelf.

Opstartsector

Een sector aan het begin van elke schijf die de architectuur van de schijf identificeert (sectorgrootte, clustergrootte, enz). Bij opstartdiskettes bevat de opstartsector ook een programma dat het besturingssysteem laadt.

Opstartsectorvirus

Een bedreiging die de opstartsector van een vaste schijf of een diskette infecteert. Wanneer u probeert op te starten vanaf een diskette die geïnfecteerd is met een opstartsectorvirus, zal de bedreiging actief worden in het geheugen. Wanneer u vanaf dat ogenblik uw systeem opstart, zal de bedreigingen telkens in het geheugen geactiveerd zijn.

Pad

De exacte weg naar een bestand op een computer. Deze weg wordt doorgaans beschreven door middel van het hiërarchische archiveringssysteem vanaf het begin.

De route tussen twee willekeurige punten, zoals het communicatiekanaal tussen twee computers.

Phishing

Het onder valse voorwendselen verzenden van een e-mail aan een gebruiker, waarbij de indruk wordt gewekt dat het bericht afkomstig is van een bestaande onderneming, in een poging de gebruiker persoonlijke gegevens te ontfutselen die zullen worden gebruikt voor identiteitsroof. In het e-mailbericht wordt de gebruiker doorverwezen naar een website waar persoonlijke gegevens kunnen worden bijgewerkt, zoals wachtwoorden en creditcard-, sofi- en bankrekeningnummers, die reeds in het bezit zijn van de rechtmatige organisatie. De website is echter nep en alleen opgezet om de gebruikersgegevens te stelen.

Photon

Photon is een vernieuwende, niet opdringerige Bitdefender technologie, ontworpen om de invloed van uw beveiligingsoplossing op de prestaties te beperken. Door de activiteit van uw pc's op de achtergrond te bewaken, maakt het gebruikspatronen die helpen opstart- en scanprocessen te optimaliseren.

Polymorf virus

Een bedreiging die zijn vorm wijzigt bij elk bestand dat het infecteert. Aangezien ze geen consequent binair patroon hebben, zijn dergelijke bedreigingen moeilijk te identificeren.

Poort

Een interface op een computer waarop u een apparaat kunt aansluiten. PC's hebben verschillende types poorten. Intern zijn er verschillende

poorten voorzien voor het aansluiten van schijfstations, beeldschermen en toetsenborden. Extern beschikken PC's over poorten voor het aansluiten van modems, printers, muizen en andere randapparatuur.

Bij TCP/IP- en UDP-netwerken, zijn ze een eindpunt voor een logische verbinding. Het poortnummer duidt aan over welk type poort het gaat. Poort 80 wordt bijvoorbeeld gebruikt voor HTTP-verkeer.

Ransomware

Ransomware is een kwaadaardig programma dat geld probeert te verdienen van gebruikers door hun kwestbare systemen af te sluiten. CryptoLocker, CryptoWall en TeslaWall zijn enkele varianten die jagen op persoonlijke systemen van gebruikers.

De infectie kan verspreid worden door spam-e-mail te openen, e-mailbijlagen te openen of toepassingen te installeren zonder dat de gebruiker weet wat er op zijn systeem gaande is. Dagelijkse gebruikers en bedrijven vormen een doelwit voor ransomwarehackers.

Rapportbestand

Een bestand dat de acties weergeeft die zich hebben voorgedaan. Bitdefender houdt een rapportbestand bij met het gescande pad, het aantal gescande mappen, archieven en bestanden, en het aantal gevonden geïnfecteerde en verdachte bestanden.

Rootkit

Een rootkit is een set softwarehulpprogramma's die toegang biedt tot een systeem op beheerniveau. Deze term werd voor het eerst gebruikt voor UNIX-besturingssystemen en verwees naar opnieuw gecompileerde hulpprogramma's die indringers beheerrechten verleende, zodat ze hun aanwezigheid konden verbergen zodat ze onzichtbaar bleven voor systeembeheerders.

De belangrijkste rol van rootkits is het verbergen van processen, bestanden, aanmeldingen en logboeken. Ze kunnen ook gegevens onderscheppen van terminals, netwerkverbindingen of randapparaten als ze de geschikte software bevatten.

Rootkits zijn in wezen niet kwaadaardig. Systemen en zelfs sommige toepassingen verbergen kritieke bestanden met de hulp van rootkits. Ze worden echter het vaakst gebruikt om bedreigingen of de aanwezigheid van een indringer op het systeem te verbergen. In combinatie met

bedreigingen, vormen rootkits een ernstige bedreiging voor de integriteit en beveiliging van een systeem. Ze kunnen het verkeer controleren, achterpoortjes in het systeem maken, bestanden en logboeken wijzigen en detectie vermijden.

Schijfstation

Dit is een apparaat dat gegevens leest van en schrijft naar een schijf.

Een harde-schijfstation leest en schrijft harde schijven.

Een diskettestation opent diskettes.

Schijfstations kunnen intern (binnen de behuizing van een computer) of extern zijn (in een afzonderlijke behuizing die op de computer wordt aangesloten).

Script

Script, een andere term voor een macro of batchbestand, is een lijst opdrachten die kunnen worden uitgevoerd zonder tussenkomst van de gebruiker.

Spam

Elektronische junkmail of berichten van junknieuwsgroepen. Algemeen bekend als ongewenste e-mail.

Spyware

Elke software die heimelijk gebruikersgegevens verzamelt via de internetverbinding van de gebruikers zonder dat hij/zij zich hiervan bewust is, doorgaans voor reclamedoeleinden. Spywaretoepassingen worden doorgaans gebundeld als een verborgen onderdeel van freeware- of sharewareprogramma's die kunnen worden gedownload van het internet. We moeten echter wel vermelden dat de meeste shareware- en freewaretoepassingen geen spyware bevatten. Zodra de spyware is geïnstalleerd, worden de activiteiten van de gebruiker op het internet gevolgd en wordt deze informatie op de achtergrond naar iemand anders doorgestuurd. Spyware kan ook informatie verzamelen over e-mailadressen en zelfs wachtwoorden en creditcardnummers.

Spyware is vergelijkbaar met een Trojaans paard omdat gebruikers ook in dat geval het product onbewust installeren wanneer ze een ander programma installeren. Een veel voorkomende manier om slachtoffer te worden van spyware is bepaalde P2P-bestandsuitwisselingsprogramma's te downloaden.

Naast het feit dat deze methode onethisch is en een inbreuk op de privacy van de gebruiker betekent, steelt spyware van de gebruiker door de geheugenbronnen van de computer te gebruiken en bandbreedte te verbruiken wanneer de informatie naar de thuisbasis van de spyware wordt verzonden via de internetverbinding van de gebruiker. Aangezien spyware geheugen- en systeemgeheugen gebruikt, kunnen de toepassingen die op de achtergrond worden uitgevoerd leiden tot systeemfouten of een algemene systeeminstabiliteit.

Systeemvak

Het systeemvak, dat met Windows 95 werd ingevoerd, bevindt zich in de taakbalk van Windows (doorgaans onderaan naast de klok) en bevat miniatuurpictogrammen die systeemfuncties zoals fax, printer, modem, volume en meer, gemakkelijk toegankelijk maken. Dubbelklik of klik met de rechtermuisknop op een pictogram om de details en de besturingselementen te bekijken en te openen.

TCP/IP

Transmission Control Protocol/Internet Protocol - Een reeks netwerkprotocollen, wijdverspreid gebruikt op het internet, die communicatie bieden tussen onderling verbonden computernetwerken met verschillende hardware-architecturen en diverse besturingssystemen. TCP/IP bevat standaarden voor de manier waarop computers communiceren en regels voor het aansluiten van netwerken en het routeren van het verkeer.

Trojaans paard

Een destructief programma dat zich voordoet als een goedaardige toepassing. In tegenstelling tot kwaadaardige softwareprogramma's en wormen, vermenigvuldigen Trojaanse paarden zich niet, maar ze kunnen even vernietigend zijn. Een van de meest verraderlijke bedreigingstypes van de Trojaanse paarden is een programma dat beweert dat het uw computer kan bevrijden van bedreigingen, maar dat in werkelijkheid bedreigingen op uw computer installeert.

De term komt uit een verhaal uit de Illias van Homerus, dat vertelt over de Grieken die hun vijanden, de Trojanen een reusachtig houten paard schonken, zogenaamd als een vredesgebaar. Maar nadat de Trojanen het paard binnen de stadsmuren hadden gesleept, kwamen de Griekse soldaten, die in de holle romp van het paard verborgen zaten te voorschijn

en openden ze de poorten van de stad, zodat hun landgenoten Troje konden binnendringen en veroveren.

Update

Een nieuwe versie van een software- of hardwareproduct, dat werd ontwikkeld om een oudere versie van hetzelfde product te vervangen. Daarnaast zullen de installatieroutines voor updates vaak controleren of er reeds een oudere versie van het product op uw computer is geïnstalleerd. Is dat niet het geval, dan kunt u de update niet installeren.

Bitdefender heeft zijn eigen updatefunctie waarmee u handmatig kunt controleren op updates of die het product automatisch kan updaten.

Vals positief

Doet zich voor wanneer een scanner een bestand ten onrechte beschouwt als geïnfecteerd.

Virtueel PrivéNetwerk (VPN)

Dit is een technologie die een tijdelijke en versleutelde rechtstreekse verbinding met een zeker netwerk over een minder beveiligd netwerk mogelijk maakt. Op die manier is het verzenden en ontvangen van data veilig en versleuteld, zodat ze moeilijk te vangen is door spionnen. Een bewijs van veiligheid is de authentificatie, die enkel mogelijk is via een gebruikersnaam en wachtwoord.

Woordenboekaanval

Aanval via raden van wachtwoord, gebruikt om in te breken in een computersysteem door een combinatie van veel voorkomende woorden in te geven om zo mogelijke wachtwoorden te genereren. Dezelfde methode wordt gebruikt om decryptiesleutels van versleutelde berichten of documenten te raden. Woordenboekaanvallen slagen in hun opzet omdat veel mensen korte wachtwoorden gebruiken die uit slechts één woord bestaan en die makkelijk te raden zijn.

Worm

Een programma dat zich verspreidt via een netwerk en zichzelf ondertussen reproduceert. Dit type kan zich niet vasthechten aan andere programma's.